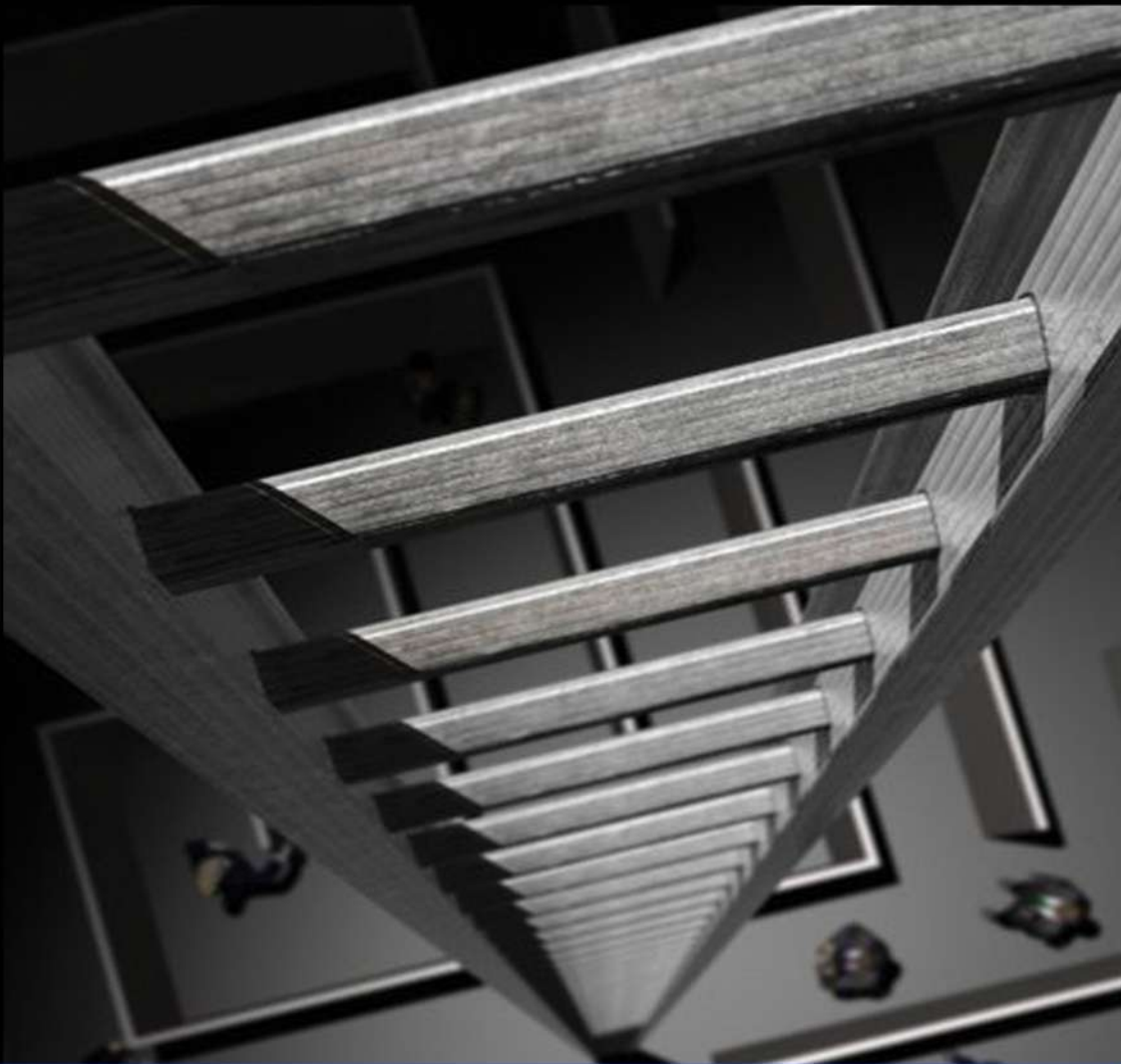


Business Continuity Management Specialist Series



A Manager's Guide

to Implement Your
IT Disaster Recovery Plan

DR GOH MOH HENG

About The Author

Dr Goh Moh Heng is the Managing Director of GMH Continuity Architects. Armed with his primary areas of expertise, which include business continuity (BC) management, disaster recovery planning, contingency planning and crisis management, Moh Heng has helped many organizations, particularly those operating in the Asia Pacific Region. Prior to establishing GMH Continuity Architects, Moh Heng held senior positions with a number of large organizations.



During his career with the Government of Singapore Investment Corporation, he was responsible for all aspects of its BC and contingency planning. At Standard Chartered Bank, he saw to the global implementation of its BC management and planning. He also managed the BC practice at PriceWaterhouse (Coopers).

Professionally, Moh Heng is the President of Business Continuity Management (BCM) Institute. He was previously the Executive Director of Disaster Recovery Institute (DRI) Asia, the Asian representation for DRI International. He was a member of the Certification Commission of DRI International, US, and was responsible for bringing DRI International's BC professional certification to Asia. Moh Heng founded the Business Continuity Group, a Technology Industry Chapter of the Singapore-based Singapore Computer Society and was its President from 1996 to 1999. Moh Heng also headed the development team responsible for developing the Singapore Standard (SS507:2004) for Business Continuity/Disaster Recovery (BC/DR) service providers and the Technical Reference (TR19:2005) for BCM in Singapore.

Moh Heng is the Senior Advisor to the China BCM Forum, a quasi government agency responsible for BCM throughout China. Moh Heng holds a doctorate from the the University of South Australia. His thesis explored the development of action learning as a contributing tool for BCM. He also holds a Master of Business in Information Technology and a B.Sc. in Computer Science. Moh Heng attended the International Management Program at INSEAD Euro-Asia Center, Fontainebleau, France. Moh Heng is an Adjunct Associate Professor with Central Queensland University and a Visiting Fellow to the Graduate College of Management, Southern Cross University, Australia. He is a Business Continuity Certified Expert (BCCE) from BCMI, a Certified Information Systems Auditor (CISA), a Fellow of the Business Continuity Institute (FBCI), UK, and a Certified Business Continuity Professional (CBCP), US.

Moh Heng regularly publishes business continuity related journals and makes presentations on business continuity management and crisis management at technical and business forums globally. He has been interviewed by BBC, ChannelNewsAsia, CNET, The Straits Times and The Economist and has been quoted by many periodicals and newspapers in Canada, India, China, Taiwan, Korea, Singapore, Philippines, Malaysia and Hong Kong.

BUSINESS CONTINUITY MANAGEMENT SPECIALIST SERIES



A MANAGER'S GUIDE TO IMPLEMENT YOUR IT DISASTER RECOVERY PLAN

Dr Goh Moh Heng PhD



www.bcm-institute.org

Published by **GMH Pte Ltd**

Produced in Singapore by WEOWNA Enterprise Pte Ltd

First Published 2007

Copyright © Mar 2016 GMH Pte Ltd

Revised 1 Mar 2016

Apart from any fair dealing for the purpose of research or private study, criticism or review, as permitted under the Copyright, Designs and Patents Act, 1988, this publication may be reproduced, stored or transmitted, in any form or by any means, only with the prior permission, in writing, of the publishers, or, in the case of reprographic reproduction, in accordance with terms of licenses issued by the Copyright Licensing Agency. Orders or enquiries concerning reproduction outside of those terms should be sent to the authority at the under-mentioned email address.

Dr. Goh Moh Heng

GMH Pte Ltd



moh_heng@GMHasia.com

moh_heng@BCM-Institute.org

ISBN 978-981-04-5975-0

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

1	OVERVIEW	15
1.1	BCM SPECIALIST SERIES	15
1.2	BUSINESS CONTINUITY MANAGEMENT (BCM)	15
1.3	BUSINESS CONTINUITY MANAGEMENT	16
1.4	DISASTER RECOVERY (DR)	16
1.5	SUMMARY OF THE DR PLANNING METHODOLOGY	17
1.6	WHY READ THIS BOOK?	18
1.7	AUDIENCE	18
1.8	BOOK STRUCTURE	19
1.9	SUMMARY OF CHAPTERS	19
2	DRIVERS FOR DISASTER RECOVERY	22
2.1	OVERVIEW	22
2.2	EMERGING TRENDS IN DR	22
2.3	TYPES OF DISASTERS	23
2.3.1	<i>Classification of Disaster</i>	23
2.3.2	<i>Classification of Disaster (Based on Driving Force)</i>	23
2.4	IMPACTS OF DISASTERS ON BUSINESS OPERATIONS	24
2.5	DAMAGE, IMPACT AND LONG-TERM EFFECTS	24
2.6	DIRECT IMPACTS	24
2.6.1	<i>Unavailability</i>	24
2.6.2	<i>Loss of Information</i>	25
2.6.3	<i>Indirect Impact</i>	25
2.6.4	<i>Long-term Impact</i>	25
2.7	WHAT ARE DR, DR PLANNING AND DR PLAN?	26
2.7.1	<i>Disaster Recovery (DR)</i>	26
2.7.2	<i>Disaster Recovery Planning (DRP)</i>	26
2.7.3	<i>Disaster Recovery Plan (DR Plan)</i>	26
2.8	NEEDS FOR A DISASTER RECOVERY PLAN	27
2.8.1	<i>Preserve Life Safety and Survival of Organization</i>	27
2.8.2	<i>Minimize Severe Losses to an Organization</i>	27
2.8.3	<i>Increase Dependency on IT</i>	28
2.8.4	<i>Raise in Customer Expectation</i>	28
2.8.5	<i>Meet Contractual Obligations</i>	28
2.8.6	<i>Maintain Effective Coordination of Recovery Tasks</i>	29
2.8.7	<i>Avoid Disaster</i>	29
2.8.8	<i>Upkeep Due Diligence and Due Care</i>	29
2.9	BENEFITS OF IMPLEMENTING A DR PLAN	29
2.9.1	<i>Ensure Continuity of Critical Component</i>	29
2.9.2	<i>Safeguard Stakeholders' Interest</i>	29
2.9.3	<i>Minimize Financial Losses</i>	30
2.9.4	<i>Identify Single Points of Failure</i>	30
2.9.5	<i>Avoid Panic During a Disaster</i>	30
2.9.6	<i>Enhance Business Processes</i>	30
2.9.7	<i>Upgrade Technology</i>	30

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

2.9.8	<i>Reduce Disruptions</i>	30
2.9.9	<i>Maintain Higher Quality Services</i>	31
2.9.10	<i>Uphold Competitive Advantage</i>	31
3	DR AND CLOUD COMPUTING	32
3.1	CLOUD COMPUTING	32
3.2	TYPES OF CLOUD	32
3.3	PRIVATE CLOUD	33
3.4	PUBLIC CLOUD	33
3.5	COMMUNITY CLOUD.....	34
3.6	HYBRID CLOUD	34
3.7	RELEVANT TO BUSINESS CONTINUITY AND DISASTER RECOVERY	34
3.7.1	<i>Cloud Deployment Model Selection Criteria</i>	34
3.7.2	<i>Selection Features for Cloud Deployment</i>	35
3.8	TYPES OF CLOUD “AS A SERVICE” MODEL.....	36
3.9	CLOUD SERVICES MODEL.....	36
3.9.1	<i>Software as a Service (SAAS)</i>	37
3.9.2	<i>Platform as a Service (PAAS)</i>	37
3.9.3	<i>Infrastructure as a Service (IaaS)</i>	37
3.9.4	<i>Recovery as a Service (RaaS)</i>	38
3.10	MANAGEMENT OF “CLOUD AS A SERVICE” PROVIDERS	39
3.11	TRADITIONAL DISASTER RECOVERY (DR)	39
3.12	DISASTER RECOVERY AS A SERVICE.....	41
3.12.1	<i>Advantages of DRaaS</i>	41
3.13	DRAAS VERSUS TRADITIONAL DR	42
4	PROJECT MANAGEMENT	43
4.1	WHAT IS PROJECT MANAGEMENT?	43
4.2	DELIVERABLES.....	43
4.3	WHAT DOES PROJECT MANAGEMENT ENTAIL?	44
4.4	STEP 1: ESTABLISH THE NEED FOR DR PLANNING	44
4.5	STEP 2: RESEARCH YOUR WORK.....	44
4.6	STEP 3: DEVELOP FRAMEWORK	45
4.7	STEP 4: DEVELOP CORPORATE DR PLANNING POLICY	45
4.8	STEP 5: DEFINE SCOPE, OBJECTIVES, AND ASSUMPTIONS.....	45
4.8.1	<i>Design Clear Objectives</i>	45
4.8.2	<i>Develop Clear Scope</i>	46
4.8.3	<i>Document Limitations and Assumptions</i>	46
4.9	STEP 6: MANAGE THE DR PLANNING PROCESS	47
4.9.1	<i>Break the Project into Phases</i>	47
4.9.2	<i>DR Project Plan</i>	47
4.10	STEP 7: ESTABLISH A STEERING COMMITTEE AND PROJECT PLANNING TEAM	47
4.10.1	<i>DR Steering Committee</i>	47
4.10.2	<i>DR Project Team</i>	48
4.10.3	<i>Clear Terms of Reference (TOR)</i>	49
4.11	STEP 8: DEVELOP AN ACTION PLAN AND SCHEDULE	49

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

4.11.1	<i>Create a Schedule</i>	49
4.11.2	<i>Get Agreement on Dates</i>	50
4.12	STEP 9: ESTABLISH A BUDGET	50
4.13	STEP 10: OBTAIN COMMITMENT AND APPROVAL.....	50
4.14	STEP 11: MANAGE DEADLINES AND MILESTONES.....	50
4.14.1	<i>Issue Recommendations After Each Phase</i>	50
4.15	STEP 12: BUILD AND MAINTAIN TEAMWORK	51
4.15.1	<i>Communicate and Participate</i>	51
5	A MANAGEMENT PROPOSAL FOR IMPLEMENTING THE DR PLAN	52
5.1	OVERVIEW	52
5.2	MANAGEMENT PROPOSAL FORMAT.....	52
5.2.1	<i>Objective and Scope</i>	52
5.2.2	<i>Historical Facts</i>	52
5.2.3	<i>Mandatory Requirements</i>	53
5.2.4	<i>In-house or External Approach</i>	53
5.2.5	<i>Resources</i>	53
5.2.6	<i>Project Schedule and Key Milestones</i>	53
5.2.7	<i>Budget</i>	53
5.2.8	<i>Key Responsibilities</i>	53
5.2.9	<i>Risks and Exposures</i>	54
5.2.10	<i>Overview of Preliminary Strategy</i>	54
5.3	QUICK ANSWERS TO COMMON ATTITUDES AND OBJECTIONS.....	54
5.3.1	<i>“Is it a problem?”</i>	54
5.3.2	<i>“We have no time for a DR Planning project.”</i>	55
5.3.3	<i>“Our insurance will cover the damage; we do not need a DR Plan.”</i>	55
5.3.4	<i>“You are spending money to satisfy the auditor.”</i>	55
5.3.5	<i>“We can still function without IT services.”</i>	55
5.3.6	<i>“The DR Plan is too expensive.”</i>	55
5.4	CONCLUSION	56
6	RISK ANALYSIS AND REVIEW	57
6.1	OVERVIEW	57
6.2	DELIVERABLES.....	58
6.3	RISK ANALYSIS	58
6.4	RISK ASSESSMENT	60
6.5	RISK TREATMENT.....	68
6.6	RISK AVOIDANCE	68
6.7	RISK REDUCTION	69
6.8	RISK TRANSFERENCE	69
6.9	RISK ACCEPTANCE	69
6.10	RISK TREATMENT PROCESS.....	69
6.11	PROCEDURAL PREVENTION.....	70
6.12	PHYSICAL PREVENTION	70
6.13	INSURANCE	70
6.14	OUTSOURCING	71

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

6.15	RECORDS KEEPING	71
6.16	OTHER CONTROL MEASURES.....	71
6.17	CONCLUSION	72
7	BUSINESS IMPACT ANALYSIS.....	74
7.1	OBJECTIVES OF BIA	74
7.2	IDENTIFY CBFs AND APPLICATIONS.....	74
7.2.1	<i>Step 1</i>	75
7.2.2	<i>Step 2</i>	75
7.3	IDENTIFY DISRUPTION IMPACTS.....	75
7.4	DEVELOP RECOVERY PRIORITIES.....	76
7.5	RECOVERY OBJECTIVES.....	76
7.6	RECOVERY POINT OBJECTIVE.....	76
7.7	RECOVERY TIME OBJECTIVE.....	77
7.8	CRITICALITY RTO/RPO TIERS	78
7.8.1	<i>RTO Tiers</i>	78
7.8.2	<i>RPO Tiers</i>	79
7.9	BIA PROCESS.....	79
7.10	BIA INITIATION.....	80
7.11	SELECT BUSINESS UNITS.....	80
7.11.1	<i>Vertical Approach</i>	80
7.11.2	<i>Horizontal Approach</i>	80
7.12	CONSIDERATIONS FOR INTERVIEWS AND QUESTIONNAIRES	81
7.13	INTERVIEW AND QUESTIONS.....	81
7.14	RESPONSE CONSOLIDATION.....	82
7.15	FINAL CONFIRMATION	82
7.16	CONCLUSION	82
8	DR STRATEGY: DATA BACKUP	89
8.1	OVERVIEW	89
8.2	PLANNING FOR DR STRATEGY	90
8.2.1	<i>Avoid (or Prevent)</i>	90
8.2.2	<i>Reduce (or Mitigate)</i>	90
8.2.3	<i>Respond/Recover or Anticipate</i>	90
8.3	BACKUP STRATEGIES	90
8.4	DATA TYPE CLASSIFICATIONS.....	91
8.4.1	<i>Application Data</i>	91
8.4.2	<i>Infrastructure Data</i>	91
8.4.3	<i>System Data</i>	92
8.5	DATA TYPES	92
8.5.1	<i>Orphan Data</i>	92
8.5.2	<i>Database Data</i>	92
8.5.3	<i>Non-Database Related Data</i>	93
8.5.4	<i>Catch-up Data</i>	93
8.5.5	<i>Lost Data</i>	93
8.6	DATA SAFETY CLASSIFICATIONS.....	93

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

8.6.1	<i>Unsafe</i>	93
8.6.2	<i>Safe</i>	93
8.7	DATA CRITICALITY CLASSIFICATION	94
8.7.1	<i>Critical Data</i>	94
8.7.2	<i>Vital Data</i>	94
8.7.3	<i>Sensitive Data</i>	94
8.7.4	<i>Non-critical Data</i>	94
8.8	TYPES OF DATA BACKUP STRATEGY	95
8.8.1	<i>Full Backup</i>	95
8.8.2	<i>Incremental Backup</i>	95
8.8.3	<i>Differential Backup</i>	95
8.8.4	<i>Online Data Backup</i>	95
8.8.5	<i>DBMS Data Log Backup</i>	95
8.8.6	<i>Mirror Backup</i>	96
8.8.7	<i>Hot Backup</i>	96
9	DR PROTECTION STRATEGY	97
9.1	DATA PROTECTION AND RECOVERY STRATEGY	97
9.1.1	<i>Data Backups</i>	97
9.1.2	<i>Replication</i>	97
9.1.3	<i>Mirroring</i>	98
9.1.4	<i>Resilient Storage Implementation</i>	98
9.1.5	<i>Cloud-based Disaster Recovery</i>	98
9.2	DATA BACKUP (MANUAL AND ELECTRONIC).....	98
9.2.1	<i>Physical Offsite Vaulting or Manual Transfer</i>	98
9.2.2	<i>Electronic Vaulting</i>	99
9.2.3	<i>Remote Tape Vaulting</i>	99
9.3	REPLICATION	99
9.3.1	<i>Synchronous Replication</i>	100
9.3.2	<i>Asynchronous Replication</i>	101
9.3.3	<i>Data Replication</i>	102
9.3.4	<i>Database Replication</i>	102
9.4	MIRRORING.....	102
9.4.1	<i>Data Mirroring</i>	102
9.4.2	<i>Disk Mirroring</i>	103
9.4.3	<i>Remote Mirroring</i>	103
9.4.4	<i>Remote Journaling</i>	103
9.4.5	<i>Database Shadowing</i>	103
9.5	RESILIENT STORAGE IMPLEMENTATION	104
9.5.1	<i>Redundant Arrays of Independent Disks (RAID)</i>	104
9.5.2	<i>Virtualization</i>	104
9.5.3	<i>Cluster</i>	105
9.5.4	<i>Network Attached Storage</i>	105
9.5.5	<i>Storage Area Network</i>	105
9.6	CLOUD-BASED DISASTER RECOVERY	106
9.6.1	<i>Do-It-Yourself</i>	106

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

9.6.2	<i>Disaster Recovery as a service or DRaaS</i>	106
9.6.3	<i>Cloud-to-Cloud DR</i>	107
9.7	DATA RECOVERY PROCESS	107
9.8	OFFSITE DATA STORAGE OPTIONS.....	108
9.9	CONCLUSION	109
10	DR STRATEGY: ALTERNATE SITES	110
10.1	ALTERNATE SITES OPTIONS.....	110
10.2	DEDICATED SITE	110
10.3	RECIPROCAL SITE	111
10.4	ALTERNATE SITES RECOVERY STRATEGY	111
10.5	COLD SITE	111
10.6	WARM SITE	112
10.7	HOT SITE.....	112
10.8	MOBILE SITE.....	113
10.9	DIFFERENCES IN ALTERNATE SITE RECOVERY STRATEGY.....	113
10.10	ADOPTION CONSIDERATIONS.....	114
10.11	EQUIPMENT REPLACEMENT STRATEGIES.....	114
10.11.1	<i>Formalize SLA of Critical Applications</i>	114
10.11.2	<i>Warehousing of Critical Equipment</i>	115
10.11.3	<i>Leverage on Compatible Equipment</i>	115
10.11.4	<i>Crate and Ship of Critical Equipment</i>	115
10.12	CONCLUSION	115
11	TENDER EVALUATION AND AWARD OF DR SERVICES.....	117
11.1	OVERVIEW.....	117
11.2	A COMPLETE RFP LIFECYCLE	118
11.2.1	<i>Pre-RFP Stage</i>	118
11.2.2	<i>RFP Development Stage</i>	119
11.2.3	<i>Distribution of RFP Document</i>	119
11.2.4	<i>Establish Deadline for RFP Proposal Submission</i>	119
11.2.5	<i>Review and Shortlist RFP Proposals</i>	119
11.2.6	<i>Schedule Vendor Presentation</i>	120
11.2.7	<i>Review and Award the RFP</i>	120
11.2.8	<i>Notify Vendor of RFP Results</i>	120
11.2.9	<i>Finalize the Award</i>	120
11.2.10	<i>Post-RFP Stage</i>	120
11.3	MAJOR COMPONENTS OF THE RFP DOCUMENT.....	120
11.3.1	<i>Administration Instruction</i>	121
11.3.2	<i>Time Requirements</i>	121
11.3.3	<i>Location for RFP Submission</i>	121
11.3.4	<i>Respond Format</i>	121
11.3.5	<i>Pricing Structure</i>	121
11.3.6	<i>Contact Point</i>	121
11.4	OTHER ADMINISTRATIVE DETAILS.....	121
11.4.1	<i>Presentation of Proposal</i>	122

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

11.4.2	<i>Rights of the Organization</i>	122
11.4.3	<i>RFP Decision</i>	122
11.4.4	<i>RFP Preparation Costs</i>	122
11.4.5	<i>Ownership of RFP and Submitted Proposals</i>	122
11.4.6	<i>Presentation and Demonstrations</i>	122
11.4.7	<i>Verification of Qualification</i>	123
11.4.8	<i>Terms and Conditions</i>	123
11.5	INTRODUCTION TO RFP	123
11.5.1	<i>Corporate Overview</i>	123
11.5.2	<i>Scope of Services</i>	124
11.5.3	<i>Requirements</i>	124
11.5.4	<i>Business Specification</i>	124
11.5.5	<i>Technical Specification</i>	124
11.5.6	<i>Qualifications</i>	125
11.6	REFERENCES	125
11.7	RFP EVALUATION	125
11.7.1	<i>Legal Requirements</i>	126
11.7.2	<i>Business and Technical Requirements</i>	126
11.7.3	<i>Qualification</i>	126
11.7.4	<i>Cost</i>	127
11.7.5	<i>RFP Award</i>	127
12	PLAN DEVELOPMENT	129
12.1	OVERVIEW	129
12.2	PLANNING CONSIDERATIONS FOR PLAN DEVELOPMENT	130
12.3	DISASTER RECOVERY TEAMS	130
12.3.1	<i>DR Management Team</i>	130
12.3.2	<i>Business Recovery Teams (Non-IT)</i>	131
12.3.3	<i>Disaster Recovery Teams (IT)</i>	131
12.3.4	<i>Staff Selection Criteria</i>	132
12.4	DISASTER RECOVERY LIFE CYCLE	133
12.5	COMPONENTS OF A DR LIFE CYCLE	133
12.5.1	<i>Reduce</i>	134
12.5.2	<i>Response</i>	134
12.5.3	<i>Recover</i>	134
12.5.4	<i>Re-sync</i>	135
12.5.5	<i>Resume</i>	135
12.5.6	<i>Return</i>	135
12.6	TIMING OF DR LIFE CYCLE	135
12.7	GENERAL INFORMATION	136
12.7.1	<i>Purpose</i>	136
12.7.2	<i>Scope</i>	136
12.7.3	<i>Information Classification</i>	136
12.7.4	<i>History of Changes</i>	137
12.7.5	<i>Organization Chart</i>	137
12.7.6	<i>Overview of DR Plan</i>	137

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

12.8	REDUCTION STAGE.....	137
12.9	RESPOND STAGE.....	137
12.9.1	<i>Notification Procedures</i>	138
12.9.2	<i>Notification Contact List</i>	140
12.9.3	<i>Damage Assessment</i>	141
12.9.4	<i>Plan Activation</i>	142
12.10	RE-SYNC AND RECOVERY STAGES.....	143
12.10.1	<i>Sequence of Recovery Activities</i>	143
12.10.2	<i>Recovery Procedures</i>	143
12.11	RETURN STAGE.....	145
12.11.1	<i>Original Site is Beyond Recovery</i>	145
12.11.2	<i>Recovering from a Damaged Original Site</i>	145
12.11.3	<i>Restoration</i>	146
12.11.4	<i>Confirm the Operational Readiness of the Original Site</i>	146
12.12	APPENDICES FOR DR PLAN.....	147
12.12.1	<i>Criteria for Appendices</i>	147
12.12.2	<i>Benefits of Appendices</i>	147
12.12.3	<i>Common Appendices Items</i>	147
12.13	CONCLUSION.....	148
13	TESTING AND EXERCISING.....	149
13.1	OVERVIEW.....	149
13.2	PRE-TEST PLANNING ACTIVITIES.....	150
13.3	DEFINE SCOPE AND OBJECTIVES FOR TEST.....	150
13.4	DESIGN TEST SCENARIO.....	150
13.5	DR PLAN TEST CYCLE.....	151
13.5.1	<i>Checklist Test</i>	151
13.5.2	<i>Paper Test</i>	151
13.5.3	<i>Walkthrough Test</i>	151
13.5.4	<i>Phase Approach or Unit Test</i>	151
13.5.5	<i>Cutover or Parallel Test</i>	152
13.5.6	<i>Full Interruption Test</i>	152
13.6	DESIGN THE KEY SUCCESS MEASUREMENT FOR TEST.....	152
13.7	DESIGN OF OTHER KEY TEST COMPONENTS.....	152
13.8	CONTENT OF A FINALIZED TEST PLAN.....	153
13.8.1	<i>Execution of Test</i>	153
13.8.2	<i>Managing Test Activities in Test</i>	153
13.8.3	<i>Managing Users in DR Test</i>	154
13.8.4	<i>Managing Problems in Test</i>	154
13.8.5	<i>Managing Risk to Normal Operations in Test</i>	154
13.9	POST-TEST REVIEW AND DOCUMENTATION.....	154
13.9.1	<i>Consider Major Tasks</i>	154
13.9.2	<i>Guidelines for Establishing the Post-test Review Document</i>	155
14	PROGRAM MANAGEMENT.....	156
14.1	OVERVIEW.....	156

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

14.2	MAJOR CONSIDERATIONS FOR MAINTAINING DR PLAN	157
14.3	PLAN MAINTENANCE PROCESS	157
14.3.1	<i>Define Clear Accountability of Individuals to Maintain Respective Procedures</i>	157
14.3.2	<i>Change Management Process</i>	157
14.3.3	<i>Periodic Inspection and Assessment Programs</i>	158
14.4	PLAN DISTRIBUTION PROCESS.....	158
14.5	MAKE A MULTI-YEAR INVESTMENT IN RECOVERY	159
15	PROGRAM MANAGEMENT: AWARENESS AND TRAINING.....	160
15.1	OVERVIEW.....	160
15.2	AWARENESS AND TRAINING APPROACH	160
15.3	AWARENESS AND TRAINING PROGRAM DEVELOPMENT PROCESS	161
15.3.1	<i>Analysis</i>	161
15.3.2	<i>Sourcing</i>	161
15.3.3	<i>Development</i>	161
15.3.4	<i>Delivery</i>	161
15.3.5	<i>Evaluation</i>	162
15.4	CONSIDERATIONS FOR AWARENESS AND TRAINING PROGRAMS	162
15.5	AWARENESS PROGRAMS.....	162
15.5.1	<i>Annual Training Plan</i>	162
15.5.2	<i>New Employee Orientation Program</i>	163
15.5.3	<i>Posters and Notices</i>	163
15.6	TRAINING PROGRAMS	163
15.7	PRE-PLANNING PHASE.....	163
15.8	PROJECT MANAGEMENT PHASE.....	163
15.9	PLAN DEVELOPMENT PHASE.....	164
15.10	TESTING AND EXERCISE PHASE	164
15.11	PROGRAM MANAGEMENT PHASE	165
15.12	CONCLUSION	165
16	REFERENCES.....	166
17	APPENDIX A - TECHNICAL DR CONSIDERATIONS - END USER COMPUTING	170
17.1	OVERVIEW.....	170
17.1.1	<i>Fixed Based Computing</i>	170
17.1.2	<i>Mobile Computing</i>	170
17.2	TECHNICAL DR CONSIDERATIONS.....	170
17.2.1	<i>Encourage Individuals to Backup Data Regularly</i>	170
17.2.2	<i>Store Backups Offsite</i>	171
17.2.3	<i>Provide Guidance on Saving Data on Personal Computers</i>	171
17.2.4	<i>Standardized Hardware, Software, and Peripherals</i>	171
17.2.5	<i>Document System Configurations and Vendor Information</i>	171
17.2.6	<i>Alignment With Organisation’s Network Security and System Access Security Policy</i>	171
17.3	CONSIDERATIONS FOR CHOOSING DR SOLUTIONS.....	171
17.3.1	<i>Equipment Interoperability</i>	172
17.3.2	<i>Storage Volume / Data Size</i>	172

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

17.3.3	<i>Media Life</i>	172
17.3.4	<i>Backup Software</i>	172
17.4	DATA BACKUP MEDIA	172
17.4.1	<i>Portable Drives</i>	172
17.4.2	<i>Tape Drives</i>	172
17.4.3	<i>Removable Cartridges</i>	173
17.4.4	<i>DVD & CD-ROM</i>	173
17.4.5	<i>Network Storage</i>	173
17.4.6	<i>Disk Imaging</i>	173
17.4.7	<i>Power Supplies</i>	173
18	APPENDIX B - TECHNICAL DR CONSIDERATIONS – SERVERS	175
18.1	OVERVIEW.....	175
18.2	DR CONSIDERATION	175
18.2.1	<i>Offsite Storage for Backup Media</i>	175
18.2.2	<i>Standardized Hardware and Software</i>	176
18.2.3	<i>Special Agreement with Manufacturer</i>	176
18.2.4	<i>System Configurations and Vendor Information</i>	176
18.2.5	<i>Alignment with Security Policy</i>	176
18.3	DR SOLUTIONS.....	176
18.4	SYSTEM BACKUP METHODOLOGY.....	177
18.5	QUALITY OF STORAGE MEDIA	177
18.6	OFFSITE MEDIA STORAGE	177
18.7	RESILIENCY TECHNOLOGIES.....	178
18.7.1	<i>RAID</i>	178
18.7.2	<i>Clustering</i>	178
18.7.3	<i>Remote Journaling and Electronic Tape Vaulting</i>	179
18.7.4	<i>Data Replication</i>	179
18.8	STORAGE VIRTUALIZATION	180
19	APPENDIX C - TECHNICAL DR CONSIDERATIONS – LOCAL AREA NETWORKS	181
19.1	OVERVIEW.....	181
19.2	DR CONSIDERATIONS	182
19.2.1	<i>Network Diagrams and Configuration Information</i>	182
19.2.2	<i>Vendors Contacts</i>	182
19.2.3	<i>Alignment with Organisation's Network Security and System Access Security Policy</i>	182
19.3	CONSIDERATIONS FOR CHOOSING DR SOLUTIONS.....	182
19.3.1	<i>Identify Single Points of Failure</i>	182
19.3.2	<i>Identify Network Connection Points</i>	183
19.3.3	<i>Remote Accessibility</i>	183
19.3.4	<i>Wireless Connectivity</i>	183
19.3.5	<i>Network Monitoring Software</i>	183
20	APPENDIX D - TECHNICAL DR CONSIDERATIONS - WIDE AREA NETWORKS.....	184
20.1	OVERVIEW.....	184

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

20.2	DIAL-UP	184
20.3	ISDN.....	184
20.4	DSL.....	184
20.4.1	<i>Leased Lines</i>	184
20.4.2	<i>ATM</i>	185
20.4.3	<i>Frame Relay</i>	185
20.4.4	<i>SONET</i>	185
20.4.5	<i>Wireless</i>	185
20.4.6	<i>VPN</i>	185
20.5	TECHNICAL DR CONSIDERATIONS.....	185
20.5.1	<i>Technical Documentation</i>	186
20.6	DR SOLUTIONS.....	186
20.6.1	<i>Redundancy of Communications Links</i>	186
20.6.2	<i>Redundancy of Network Connecting Devices</i>	187
20.6.3	<i>Redundancy of Network Service Providers</i>	187
20.6.4	<i>Tighten Service Level Agreements with Network Service Providers</i>	187
21	APPENDIX E: A SAMPLE TABLE OF CONTENTS OF DR PLAN	188
21.1	EXPLANATION	188
22	APPENDIX F: A SAMPLE DR PLAN.....	192
22.1	EXPLANATION	192
22.2	INTRODUCTION	192
22.3	OVERVIEW.....	192
22.4	PURPOSE.....	192
22.5	SCOPE.....	193
22.5.1	<i>Scope of the Plan</i>	193
22.5.2	<i>Assumptions</i>	193
22.6	RESPONSIBILITY	194
22.7	AUTHORIZATION.....	195
22.7.1	<i>Plan Review and Approval</i>	195
22.7.2	<i>Authority to Invoke DR Plan</i>	195
22.8	AUTHORITY/REFERENCES.....	195
22.9	RECORD OF CHANGES.....	196
22.10	BUSINESS IMPACT ANALYSIS	196
22.10.1	<i>Critical Business Functions</i>	196
22.10.2	<i>IT Resource Requirements and Recovery Priority</i>	197
22.11	DISASTER RECOVERY STRATEGY AND ACTIVITIES.....	197
22.11.1	<i>Recovery Strategy</i>	197
22.11.2	<i>Recovery Activities</i>	197
22.11.3	<i>Notification and Damage Assessment Phase</i>	198
22.11.4	<i>Damage Assessment Procedures</i>	198
22.11.5	<i>Activation Phase</i>	199
22.11.6	<i>Mobilization Phase</i>	199
22.12	RECOVERY PHASE	199
22.12.1	<i>Recovery Goal (RTO 6 to 8 hours)</i>	200

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

22.12.2	Recovery Goal (RTO 8 to 24 hours)	200
22.12.3	Recovery Goal (RTO 24 to 48 hours)	200
22.13	RETURN TO NORMAL OPERATIONS	200
22.13.1	Original or New Site Restoration	200
22.14	CONCURRENT PROCESSING	201
22.15	PLAN DEACTIVATION	201
22.16	TESTING STRATEGY	201
22.16.1	Test Scope	201
22.16.2	Test Approach	201
22.16.3	Successful Test Criteria.....	202
22.17	AWARENESS AND TRAINING STRATEGY.....	202
22.17.1	Approach	202
22.17.2	Process.....	202
22.18	SCHEDULE FOR REVIEW.....	203
22.19	PLAN APPENDICES	204
23	APPENDIX G: DR PLANNING PROJECT - MAJOR ACTIVITIES / MILESTONES.....	205
23.1	EXPLANATION	205
23.2	PROJECT MANAGEMENT.....	205
23.3	RISK AND ANALYSIS REVIEW	205
23.4	BUSINESS IMPACT ANALYSIS	206
23.5	DR STRATEGY	206
23.6	PLAN DEVELOPMENT.....	206
23.7	TESTING AND EXERCISING.....	206
23.8	PROGRAM MANAGEMENT	207
23.9	PROJECT COMPLETION	207
24	APPENDIX H: DR SITE - SELECTION & EVALUATION CHECKLIST	208
24.1	EXPLANATION	208
25	APPENDIX I - A SAMPLE QUESTIONNAIRE FOR CONDUCTING BUSINESS IMPACTS ANALYSIS INTERVIEWS	212
25.1	EXPLANATION	212
26	APPENDIX J - A SAMPLE TABLE OF CONTENT OF REQUEST FOR PROPOSAL.....	218
26.1	EXPLANATION	218
26.2	TABLE OF CONTENT.....	218
27	APPENDIX K: A SAMPLE OF DR TEST CHECKLIST.....	220
27.1	EXPLANATION	220
28	APPENDIX L: A SAMPLE OF DR TEST DESIGN TEMPLATE	222
29	APPENDIX M: FREQUENTLY ASKED QUESTIONS	227
29.1	WHAT IS DRP?	227
29.2	WHAT IS THE DIFFERENCE BETWEEN THE VARIOUS PLANS?	227
29.3	WHAT IS THE CONNECTION BETWEEN RM AND DRP?	228

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

29.4	INTO WHAT PHASE OF THE SDLC SHOULD DRP BE INCORPORATED?	228
29.5	WHAT IS THE FIRST STEP I NEED TO TAKE BEFORE WRITING A DR PLAN?	228
29.6	WHICH DR SOLUTIONS SHOULD BE IMPLEMENTED TO ENSURE AVAILABILITY?	228
29.7	WHAT TYPE OF ALTERNATE SITE SHOULD I CHOOSE?	229
29.8	HOW FAR SHOULD THE ALTERNATE SITE BE FROM THE PRIMARY SITE?	229
29.9	WHEN AN EVENT OCCURS, WHO SHOULD BE NOTIFIED?	229
29.10	WHAT IS THE RESUMPTION PHASE?	229
29.11	HOW OFTEN SHOULD MY DR PLAN BE TESTED?	229
29.12	HOW OFTEN SHOULD MY DR PLAN BE UPDATED?	230
29.13	HOW ARE DR PLAN AND ITS SOLUTIONS COORDINATED?	230
30	INDEX.....	231

1 Overview

"Let our advance worrying become advance thinking and planning."

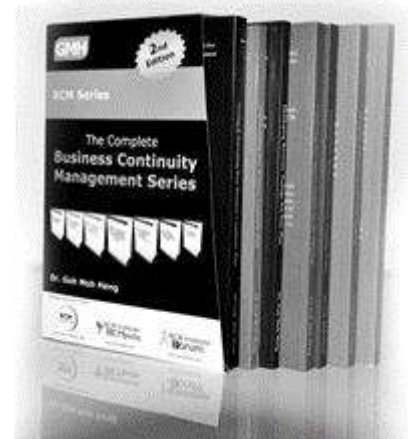
Winston Churchill

1.1 BCM Specialist Series

This book is part of the Business Continuity Management (BCM) Specialist Series. It is a series of BCM books that broaden the BCM knowledge domain. This range of this book series covers auditing, IT disaster recovery planning (DRP), the implementation of a pandemic influenza BC Plan and the implementation of standards such as SS540, BS25999 and finally, the ISO22301, crisis communication, and crisis management.

The author's previous set of books, called the BCM Series, presents a step-by-step program that aims to equip the organization with a complete understanding of the BCM Planning Methodology (**Figure 1-2**).

In addition, it provides detailed documentation, explanations, and templates of invaluable reference material. This BCM book series adopts the following BCM Planning Methodology or Process based on seven blocks of activities.



1.2 Business Continuity Management (BCM)

Business Continuity (BC) Management (**Figure 1-1**) is a holistic management process for identifying threats' potential impacts and developing response plans. The key objective is to increase an organization's resilience to business disruptions and minimise such disruptions' impact.

Potential threats can endanger the continuity of Information Technology (IT) infrastructures and business and supply chain processes. The result of applying the BCM Planning Methodology (see **Figure 1-2**) is a response or recovery plan that will minimize the debilitating impact of threats to allow the continuity of the various business processes.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

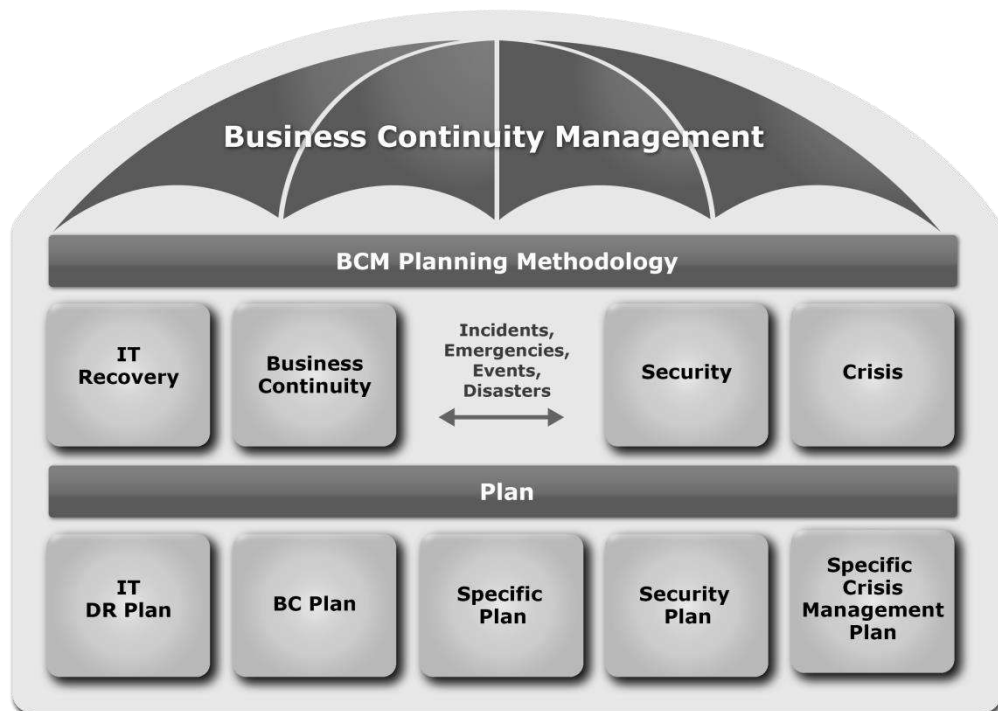


Figure 1-1: Business Continuity Management (BCM) Overview

1.3 Business Continuity Management

Business Continuity (BC) Management (Figure 1-1) is a holistic management process to identify potential impacts from threats and develop response plans. The key objective is to increase an organization's resilience to business disruptions and minimise such disruptions' impact.

Potential threats can endanger the continuity of Information Technology (IT) infrastructure and business and supply chain processes. The result of applying the BCM or "IT Disaster Recovery" (hereafter referred to as DR) planning methodology (See Figure 1-2) is a response or recovery plan that will minimize the debilitating impacts of threats to continue the various business processes. In the context of this book, DR Planning is part of Business Continuity Management.

1.4 Disaster Recovery (DR)

This DR Management book adopts the DR Planning Methodology or Process (similar to the BCM Planning Methodology) based on seven blocks of activities.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

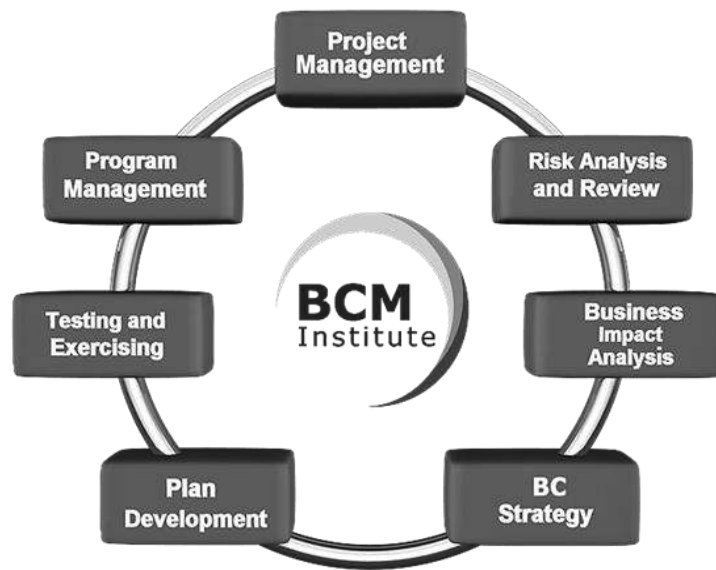


Figure 1-2: BCM Planning Methodology
(Used with permission from BCM Institute)

1.5 Summary of the DR Planning Methodology

The following summarizes each phase of the DR planning process:

Project Management

Define and organize the project planning parameters and identify the resources needed to complete the DR Plan. (Goh, 2008c)

Risk Analysis and Review

Identify existing risks and threats that the business organization can be exposed to, particularly its geographic location, processes, and procedures. (Goh, 2008a)

Business Impact Analysis

Evaluate each business unit's critical IT applications and operations and determine the resources needed to run them. (Goh, 2008b)

DR Strategy

- Develop interim recovery guidelines and procedures for business units operating in “time of disaster” and “ready for normal business.” (Goh, 2009)
- Arrange for alternate facilities and store backups of vital records in a safe place.

Plan Development

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Determine the procedures for notifying the right people, assessing the operational impact and activating the recovery. (Goh, 2010a)
- Develop specific steps to minimise the risks of an outage and restore normal operations after the outage. The output from this step is the DR Plan.

☐ **Testing and Exercising**

- Subject the developed recovery plan to tests to ensure that it works. (Goh, 2006)

☐ **Program Management**

- Update and maintain the plan constantly to reflect changed conditions in the business. (Goh, 2010b)
- Review and audit the readiness and completeness of the plan.
- Ensure that all staff members involved in the recovery process understand the recovery plan.
- Manage the overall DR program.

1.6 Why Read This Book?

This DR planning book is written to help organizations establish and maintain high DR capabilities in IT services to support their business missions. This book will provide organizations with the following objectives.

- An internationally recognized good practice DR Planning process or methodology with a strong foundation in conceptualizing, developing and maintaining an effective and efficient DR Plan.
- A structural and procedural approach to developing a DR Plan for the entire IT infrastructure and services required for its critical business applications.
- Practical DR Guidelines, considerations, practices and samples that are beneficial for DR practitioners to facilitate and manage the DR Planning process.
- Effective management justifications and DR services sourcing approach to assist new DR practitioners in initiating management support for implementing the DR Plan.

This book is handy for anyone who needs to conceptualize and develop a DR Plan. It provides an extensive framework to identify and evaluate IT risks, business impacts due to the risks, DR requirements, and prioritization. At the same time, this book follows a structural development approach that will save time and cost in developing a cost-effective DR Plan that addresses all aspects of the business requirements for IT services.

1.7 Audience

The principles presented in this book are helpful to everyone responsible for DR Planning at the system and operational levels, including:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Managers oversee IT operations or business processes that rely on IT systems.
- IT project managers, system architects, IT services outsourcers, IT services providers, DR services providers and any other personnel responsible for designing, managing, operating, maintaining, or using information systems.
- System administrators are responsible for maintaining daily IT operations.
- Users who employ desktop and portable systems to perform their assigned job functions.
- IT security officers, auditors, and other staff are responsible for developing, implementing, and maintaining an organization's IT risk management activities.

Also, this book may be used by emergency management personnel who may need to coordinate facility-level DR or continuity plans with DR Planning activities.

1.8 Book Structure

This book is designed to lead the reader logically through the process of:

- Developing a DR Planning program applicable to different types of organizations.
- Evaluating an organization's needs against recovery strategy options and technical considerations.
- Documenting the strategy into a DR Plan.
- Verifying the effectiveness and correctness of the DR Plan.
- Maintaining and updating the DR Plan to reflect its applicability during unexpected disasters.

The DR Plan serves as a "user manual" for executing the strategy during a disruption. Therefore, illustrative examples have been included, wherever possible, to give the reader a better understanding.

1.9 Summary of Chapters

The following gives a preview of the subsequent sections of this book as well as what each section covers:

☐ **Chapter 1: Overview of Business Continuity Management**

It discusses the relationship between business continuity management, business continuity planning, disaster recovery planning and crisis management. It includes how an organization would embark on implementing its DR program. The DR Planning process or methodology for developing and implementing a DR Plan is further elaborated.

☐ **Chapter 2: Drivers for DR**

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

It describes the drivers and benefits of having the DR Plan and the different degrees of impact that disasters can have on business operations.

Chapter 3: Cloud Computing and DR

It summarises the computing deployment and service models and how they relate to disaster recovery. It compares the traditional and cloud DR approach.

Chapter 4: Project Management

It provides an overview of developing a tactical plan for implementing the DR Plan.

Chapter 5: A Management Proposal for DR Plan

It consolidates a management proposal's techniques, considerations, and format for implementing a DR Plan.

Chapter 6: Risk Analysis and Review

It described the processes and building blocks to ensure all risks are thoroughly identified, assessed and reviewed.

Chapter 7: Business Impact Analysis

It introduces business impact analysis and the critical part of developing the DR Plan.

Chapter 8: Disaster Recovery Strategy

It describes the DR mechanisms and strategies and the steps to select those that match an organization's needs.

Chapter 9: Tender, Evaluation, and Award of DR Services

It elaborates on tendering and awarding DR services, the Request for Proposal (RFP) contents, and evaluating and awarding RFPs.

Chapter 10: Plan Development

It summarises the steps described in developing a DR Plan, starting with reducing, response, recovery, restoring, resuming, and returning to the primary location. It essential to have a comprehensive representation of all functions within the organization must be established.

Chapter 11: Testing and Exercising

It describes a complete walk-through of the DR Plan testing process. The process includes the key considerations and leading activities during the DR Plan testing phase.

Chapter 12: Program Management

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

This phase describes how an organization transits from project management to program management. It starts with the DR Plan maintenance process and an understanding of how to ensure the timeliness and effectiveness of the DR Plan on an on-going basis.

☐ **Chapter 13: Program Management: Awareness And Training**

It presents a full DR training and awareness lifecycle in disseminating DR knowledge to management, DR teams, and staff, the key considerations to focus on for drawing up training and awareness programs, and the main activities of the programs.

☐ **Appendices**

The specific technical considerations for DR Planning in end-user computing, servers, LANs, WANs, mainframe and distributed systems; and samples of the plan, checklist and recovery procedure to enhance understanding.



This icon will contain information that is helpful tips to the readers.

2 Drivers for Disaster Recovery

"DR is just not about the recovery of computer systems!"

Goh, Moh Heng

2.1 Overview

In our daily lives, whenever there is news reporting on a disaster, the scenes of fire, flood, hurricanes, coups, and terrorist attacks quite quickly come into mind. Although there are regions where some of these threats are more real than elsewhere, we must remember that disasters come in a variety of guises. It does not have to be a large-scale event to mean disaster for your organization. Neither does it have to be an event that causes extensive damage to the infrastructure.

Imagine, for instance, an event in your neighbourhood that requires an evacuation of the whole building until the problem is solved. This could last hours or even days. Your computers will still be running, your telephones will still be ringing, and your business infrastructure will not be damaged. However, you cannot use it. You cannot answer the telephone and cannot enter the building. Such circumstances can have disastrous consequences on your business.

Thus, disasters can come in different forms, and their impacts vary in magnitude. Therefore, we must understand them well to formulate and implement effective countermeasures.

2.2 Emerging Trends in DR

While reviewing the drivers for DR, it is helpful to understand some of the market trends in DR.

- Cloud (Computing)

Cloud Computing (Online Tech, 2015) delivers faster recovery times and multi-site availability at a fraction of the cost of traditional disaster recovery.

- Virtualization

With virtualization (Online Tech, 2015), the server, including the operating system, applications, patches and data, is encapsulated into a single software bundle or virtual server. This virtual server can then be copied or backed up to an offsite data centre and spun up on a virtual host in minutes.

- Social networking

- Managed DR
- Electronic-based vaulting
- Mobility

2.3 Types of Disasters

These are the typical classification of disasters.

2.3.1 Classification of Disaster

- Acts of nature such as hurricanes and floods.
- External man-made events such as terrorist attacks and security intrusions.
- Internal unforeseen events such as accidental loss of files and computer failure.
- Internal intentional events such as labour strikes and sabotage.

Such classifications have merits in driving emergency plans and crisis management, where the event itself must be managed to protect people and assets and mitigate the damage. However, a different set of disaster classifications may be more effective in DR Planning, where the objective is to resume IT operations to support the business.

The driving force in DR Planning should be from how an unexpected event impacts your IT support for the business operations rather than from how to eliminate risks according to the probability of an unexpected event occurrence. In other words, recovery prioritization for mission-critical IT systems and services is based on the impact of losses to the organization in the event of a disaster.

2.3.2 Classification of Disaster (Based on Driving Force)

A more typical disaster classification based on the driving force is as follows:

- Failure of an individual infrastructure element, such as a single point of failure.
- Longer-term interruption of critical information flow.
- Longer-term interruption of a chain of critical business activity or business functions.
- Longer-term interruption is affecting local businesses.
- Complete business interruption.

Based on experience has shown that, in many cases, the effect of an unexpected event cascades into more significant impact levels. This underlines why, for DR Plan to be effective, the IT DR team must be driven from the perspective of managing and minimizing impacts rather than just handling the event.

2.4 Impacts of Disasters on Business Operations

An unexpected event's immediate consequence is the damage it generates; this is where most insurance can assist you in managing a disaster. However, not the direct physical damage that is the most crucial concern, but the impact on business operations and how this can be overcome to resume the business and survive as an organization.

2.5 Damage, Impact and Long-Term Effects

An unexpected event can cause damage to infrastructure elements and resources supporting business operations. Examples are buildings, computers, and networks. The damage can be such that the infrastructure element is destroyed or unavailable for an extended period.

When preparing and implementing the DR effort, it is vital to distinguish between damage caused by the event and the impact on the business because of the unavailability or the loss of vital information.

Besides the impact on business operations, one must also consider the long-term effects of such unexpected events. These are business impacts still felt long after the business has been resumed and operations have returned to normal. Examples of loss of market share, lower share price, customer confidence, and goodwill. All these elements must be considered and will drive the DR Planning.

2.6 Direct Impacts

There are two major types of direct impacts resulting from a disaster, and they are:

- Unavailability of infrastructure and resources.
- Loss of vital information.

2.6.1 Unavailability

The unavailability of IT infrastructure has always been the focus of traditional DR Planning, which focuses mainly on replacing hardware or switching to alternative infrastructure. However, this approach is becoming scarce as it is rarely cost-justified to duplicate all the organization's resources. Deciding how far one should go in these arrangements is often challenging unless priorities are identified.

It is rarely possible to duplicate the complete business infrastructure after disaster strikes, and business operations will have to be organized with only limited infrastructure available. Therefore, executing the most critical business activities with this limited infrastructure and personnel is one of the fundamental challenges of DR Planning.

Very likely, given the limited infrastructure and resources, the information flows, and the business operations will have to be well-organized to meet the business objectives at minimum acceptable levels.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

2.6.2 Loss of Information

Typically, an organization will need to restart its recovery from the last available backup during a disaster. Such a task requires the recovery team to identify and restore all transactions entered after the last successful backup, as they will not be on the system after the restoration. As a result, the possibility of such vital data and information being lost and irrecoverable is high. Furthermore, even if the data is available, there is the possibility that data restored from different backups taken at different times may not be synchronized.

For example, the backup for order-processing data may be taken later than the backup data for the financial systems, including the accounts receivable. It is as if your organization has gone back in time, but each system is to a different time zone, and you have to match the different time zones.

In addition to the time mismatch, the business events associated with the missing transactions may already have been executed. For instance, invoices may have been sent out, goods shipped, and payments made, but there may be no trace of these events in the information system.

When analyzing the impact of information and data loss, one must consider the following:

- How can the lost information and data be retrieved?
- Can you reconstruct this information based on paper audit records, customers, suppliers or business partners?
- How long will it take to recover the data and information?
- How much effort and resources are required for the recovery?
- What will the effect be on your organization's reputation?
- How long can the business operate without mission-critical IT systems and operations?
- What problems may you face while synchronising and integrating the reconstructed data with the live data?

2.6.3 Indirect Impact

Due to the interdependencies between business units, each business process typically consists of a chain of activities executed by different business units. An unexpected event can interrupt a business activity and an information flow supporting a business process. If the event is such that one business activity cannot be executed, this could affect the entire business process and ripple through the organization. Even a relatively small event can have a tremendous impact in an environment where many activities depend on each other.

2.6.4 Long-term Impact

Usually, the long-term effects will likely be seen after the organization has recovered from a disaster and has returned to its normal business operations. The degree of impact

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

depends on how good the DR Plan is (working together with the business continuity plan). An effective and efficient DR plan will help you to recover your business quickly. Some of the long-term impacts can include:

- Loss of customers
- Weakened financial position
- Loss of market share and confidence
- Eroded public image and liabilities

2.7 What are DR, DR Planning and DR Plan?

Based on the definition from BCMpedia (BCM Institute, 2008) (http://www.bcmpedia.org/wiki/Disaster_Recovery_DR_Glossary), the following terms: disaster recovery, disaster recovery planning and disaster recovery plan are elaborated.



2.7.1 Disaster Recovery (DR)

Disaster Recovery (DR) is the ability to provide critical Information Technology (IT) and telecommunications capabilities for some predetermined minimum period by an organization disrupted by an incident, emergency or disaster. DR recovers the disrupted IT and telecommunications capabilities to ensure Critical Business Functions (CBFs) can continue to planned levels of disruption.

2.7.2 Disaster Recovery Planning (DRP)

Disaster Recovery Planning (DRP) is developing advanced arrangements and procedures that enable an organization to respond to a disaster and resume the business-critical applications within a predetermined period, minimize the amount of loss, and repair or replace the damaged facilities as soon as possible. It includes one or more of the approaches to restore disrupted IT services:

- Restore IT operations at an alternate site.
- Recover IT operations using alternate equipment.

2.7.3 Disaster Recovery Plan (DR Plan)

A Disaster Recovery Plan (DR Plan) describes how an organization deals with potential IT disasters.

Information technology (IT) and automated information systems are vital elements in most business processes and an organization's success. Therefore, it is critical that the services provided by these IT systems can operate effectively without extensive interruptions. DR Plan supports this requirement by establishing policies, procedures, processes and technical measures to recover systems efficiently and effectively following service disruptions resulting from disaster events.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

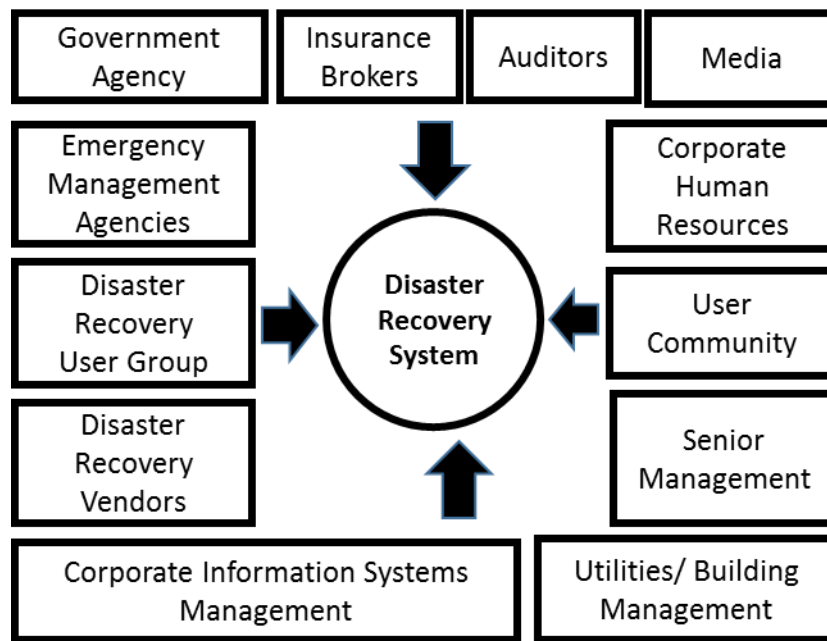


Figure 2-1: Stakeholders

2.8 Needs for a Disaster Recovery Plan

These are the essential requirements for the provision of a DR Plan.

2.8.1 Preserve Life Safety and Survival of the Organization

The most significant need for an organization to have a DR plan is to ensure the safety of the employees and the organisation's survival from a disaster. Such a plan can only be achieved through advanced planning and preparation by all stakeholders (**Figure 2-1**).

2.8.2 Minimize Severe Losses to an Organization

Depending on the nature of the work performed, an organization may lose a considerable amount of money for every hour of downtime. Typically, **Figure 2-2** shows the downtime results in the loss of revenue, customer goodwill and loss of market share. For example, an IT downtime will result in the inability to deliver customer services on time. In addition, prolonged downtime would reduce the profitability and market value of the organization and ultimately result in business failure.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

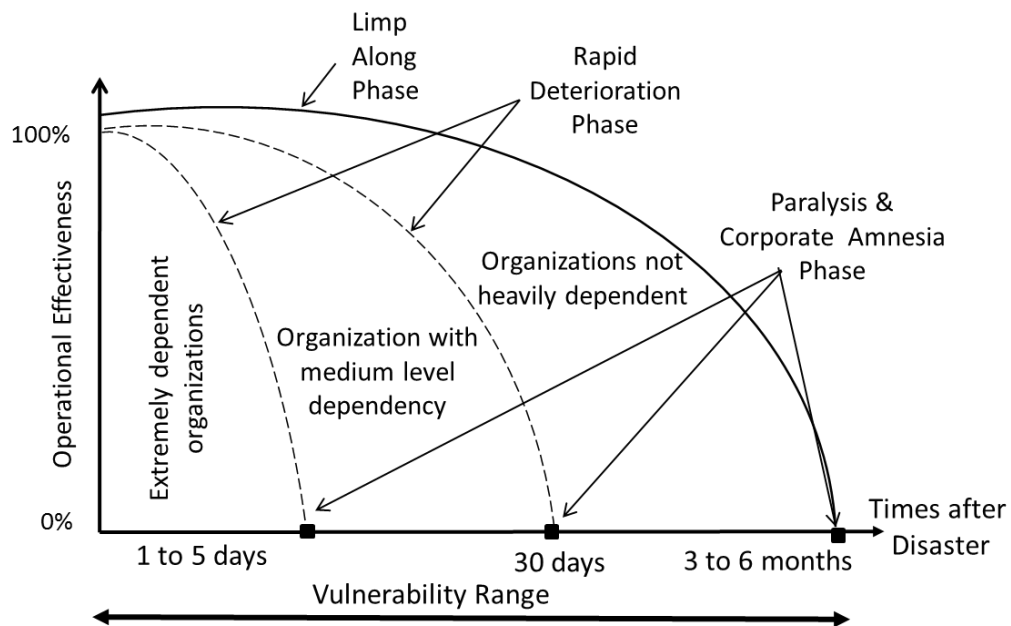


Figure 2-2: Business Deterioration after a Disaster

2.8.3 Increase Dependency on IT

There is a high dependency on IT as technology development enhances business delivery. With increased dependence on IT to deliver continuous business services, the 24-by-7 availability of IT support systems has become a fundamental requirement. Innovative methods to support these business operations are being created and implemented. However, some of these practices, such as remote connection to offices for continuous connectivity, may make an organization vulnerable to external attacks and more susceptible to disasters.

2.8.4 Raise Customer Expectations

In today's business environment, the business's survival depends on its recovery and availability within the shortest possible time. In a disaster impacting the IT setup, all the crucial functions dependent on IT, such as communication and business transactions, will be hampered. Most organizations can sustain themselves without critical IT operations for a day or two. However, any prolonged interruption can result in severe and irreparable losses to the organization, sometimes resulting in the organization becoming insolvent. Therefore, the organization can implement a DR Plan or program to ensure the recovery of its IT operations in the shortest possible time and prevent any potential calamities.

2.8.5 Meet Contractual Obligations

Organizations directly supplying products and services to customers or clients are usually bound by a Service Level Agreement (SLA) to carry out their obligations. These agreements seek assurance from the suppliers that the supply of deliverables will continue unhindered in the face of disasters. When the supplier commits to high availability and quality service, it takes special effort on the supplier's part to fulfil the

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

SLAs. A key component of such measures is designing, developing, and implementing an effective and efficient DR Plan.

2.8.6 Maintain Effective Coordination of Recovery Tasks

In a DR Plan, list the recovery procedures to ensure that the organization resumes its operations within the shortest possible time. Because the occurrence of disasters defines these procedures, the entire DR Plan reflects the effectiveness and preparedness of the organization to meet the challenges of disasters. Therefore, a pre-planned list of the recovery procedures helps to facilitate faster and more effective recovery IT operations and services during a disaster event.

2.8.7 Avoid Disaster

DR Planning often leads to improving processes and IT systems that make those processes and systems more resilient. Events that would result in a severe business interruption before you had the DR Plan in place become, in many cases, just a minor event after you enact the plan.

2.8.8 Upkeep Due Diligence and Due Care

Very few organizations have ever experienced an incident or event resulting in data loss. However, many organizations are unaware that failing to secure their information and protect data against loss can be a severe offence. If an organization fails to exercise this due care, it could face civil or criminal.

2.9 Benefits of Implementing a DR Plan

These are the main advantages of the creation of the DR Plan. It has a direct correlation with the "Need for DR."

2.9.1 Ensure Continuity of Critical Component

The most significant benefit of implementing a DR Plan is to ensure the availability and recovery of critical IT resources and systems during a disaster. In addition, it is to sustain continuous service to customers and clients. Therefore, DR Planning is considered an integral component of business continuity.



2.9.2 Safeguard Stakeholders' Interest

A DR Plan enhances organisational stability by identifying, protecting and recovering all critical resources and activities, thereby safeguarding stakeholders' interests.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

2.9.3 Minimize Financial Losses

Before rather than after a disaster, they identify recovery measures, and their implementation in a DR Plan can minimize financial losses.

2.9.4 Identify Single Points of Failure

While assessing the business functions, a significant indirect benefit of DR Planning is determining the single point of failure, revealing an operation or process with a high dependence on a single resource. As a result, if the help is affected by a disaster, the effect on the functions or processes is catastrophic to the organization. Therefore, it is essential to look at the "big picture", and identifying such points of failure can be used to estimate the risks to the organization's business functions.

2.9.5 Avoid Panic During a Disaster

DR Planning helps to reduce panic when a disaster occurs. Before a disaster, identify all the tasks required to put the affected organization back on track in the event of a disaster. As a result, all tasks that involve decision-making during the disaster will be significantly reduced, eliminating the need to plan and unnecessary investments during disaster events. It also avoids waiting for key personnel to make critical decisions during a disaster. As a result, the organization can achieve a smooth and orderly recovery within the shortest time.



2.9.6 Enhance Business Processes

Because business processes undergo such analysis and scrutiny, analysts almost can't help but find areas for improvement.

2.9.7 Upgrade Technology

Often, IT systems need to be improved to support recovery objectives resulting in the DR Plan's development. However, the attention you pay to recoverability also often makes your IT systems more consistent with each other and, hence, more efficiently and predictably managed.

2.9.8 Reduce Disruptions

As a result of improved technology, IT systems tend to be more stable than before. Also, when an organization changes system architecture to meet recovery objectives, events that used to cause outages do not do so anymore.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

2.9.9 Maintain Higher Quality Services

Because of improved processes and technologies, both internally and with customers and supply chain partners.

2.9.10 Uphold Competitive Advantage

A good DR Plan gives an organization a bragging right that may outshine competitors. Price is not necessarily the only point on which companies compete for business. A DR plan allows an organization also to claim higher availability and reliability of services.

3 DR and Cloud Computing

“Cloud computing has shifted disaster recovery to be much more cost-effective with significantly faster recovery times.”

Goh, Moh-Heng

3.1 Cloud Computing

Cloud computing is an on-demand application delivered through the internet. It has become one of the critical steps forward for any company relying on IT processes. Businesses of all industries and sizes are now looking toward Cloud computing to effectively deliver IT services to their clients and customers. With its ability to revolutionize the IT process, Cloud computing promises massive changes to the modern-day IT department, allowing them to cut down on overhead and scale IT capacity up and down rapidly. In addition, it is cost-effective, readily available, and incredibly convenient (Giffin, 2011). It is, in essence, the future of IT functions in businesses worldwide.

3.2 Types of Cloud

There are three main types of cloud deployment models (**Figure 3-1**):

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Each variant of the Cloud has its strengths and weaknesses, advantages and drawbacks. What Cloud Model an organization chooses depends on the type of industry they are in and the scope of their IT needs.

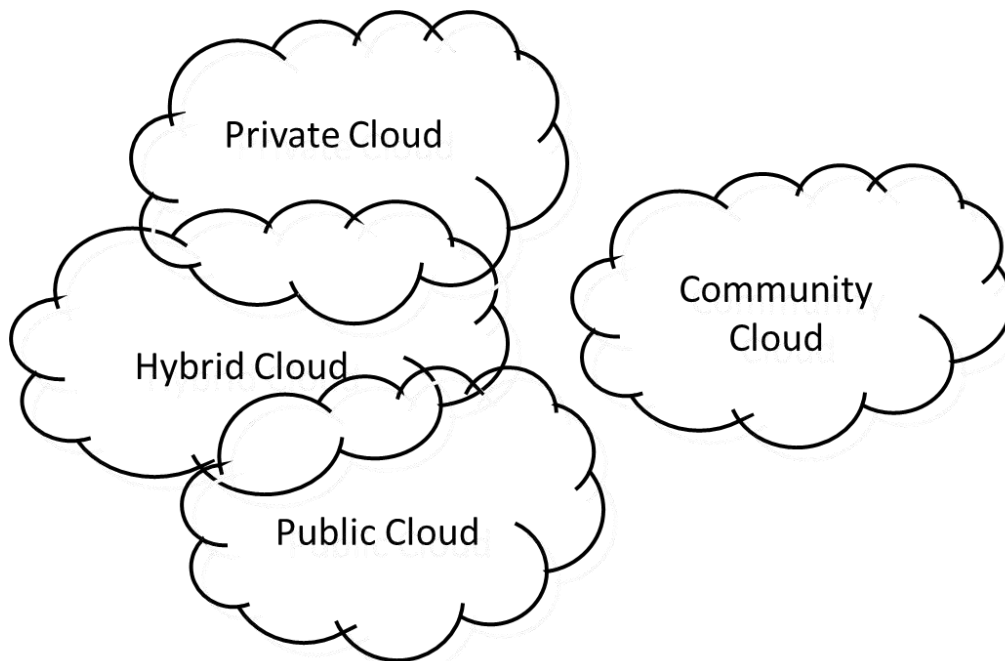


Figure 3-1: Types of Cloud

3.3 Private Cloud

The Private Cloud is intended for the single operation of a single company or organisation. It can be hosted internally or externally by the organization or outsourced to a third party. When done correctly and efficiently, hosting a private cloud can help significantly improve business – but the process it is set up could prove to be complicated.

The cloud deployment model requires the organization to reevaluate and repurpose existing resources and direct the organization to undergo major virtualization. Because of this, “virtual” types of vulnerabilities are opened up, and every step of setting up and maintaining a private cloud is, if not carefully worded, a potential security risk waiting to happen (Cloud Computing, 2015). On the other hand, one advantage of the private cloud, especially for the IT personnel managing it, is complete control over the system while adhering to the highest security standards (Welsh & Palacio, 2015).

3.4 Public Cloud

If a private cloud is, by its namesake, for private use by a single organization, then a public cloud is the exact opposite. Services on a public cloud are delivered and received over an open network available for public use. While cloud services are often cost-effective, public clouds are the only ones that are sometimes free. There are little to no vast differences between how private and public clouds function regarding IT infrastructure. However, security standards may be different. Unlike private clouds, public clouds are non-trusted networks, and most lack the security standards of private clouds (Cloud Computing, 2015).

3.5 Community Cloud

Community cloud, as defined here, has similarities to both private and public clouds. Like a private cloud, it can avoid network bandwidth, security exposures, and legal issues arising from external resources, and its use can be controlled and managed. Like a public cloud, it makes setup easy for individual organizations. It provides more efficient use of pooled resources for the whole community than its members could achieve individually (The Open Group, 2015).

3.6 Hybrid Cloud

A hybrid cloud is a mix of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. A hybrid cloud can connect collocation, managed and dedicated services with cloud resources (BTL, 2015).

3.7 Relevant to Business Continuity and Disaster Recovery

However, what does this mean for Business Continuity (BC) and, more relevantly, IT Disaster Recovery (DR)? Again, we return to Cloud Computing's greatest strength and BC and DR's most cumbersome aspect: pricing. Traditional BC and DR plans are invariably expensive, especially regarding IT Processes. The methods typically demand the purchase and maintenance of an alternative set of hardware similar to the company's existing business-critical systems. Cloud technology ensures that BC and DR professionals can access the network anywhere, even on mobile media, thanks to its constant online connections. (Gary, 2015).

The plan must also consider the business data that must be stored, the backup site to store the extra hardware, and the costs of maintaining them. Another additional cost is keeping the major hardware and the backup hardware in sync, ensuring that the backup hardware has all the data on the original hardware (Pyle, 2010). A cloud-based solution has few hardware issues as all of the software is at your fingertips. The cost-effectiveness benefits are less significant to middle-sized companies that cannot afford the enormous costs of hardware duplication that larger corporations can so quickly and readily cough up. It is, in effect, a trade-off of physical resiliency to virtual resiliency.

3.7.1 Cloud Deployment Model Selection Criteria

The selection of each cloud deployment model (Mircea & Andreescu, 2011) is based on its mission criticality and the application being core or non-core to the organization.

Business Practices	Core	Non-core
Mission-critical	Private cloud or non-cloud	Public clouds

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

Business Practices	Core	Non-core
Non-mission-critical	Private cloud or non-cloud	Public clouds

Figure 3-2: Selection of Cloud Deployment Model

3.7.2 Selection Features for Cloud Deployment

When selecting cloud deployment, these are critical features and selection criteria (Conner & Dubois, 2013).

Design and Built to Last	Security
Financial stability	Private key AES encryption
Proven infrastructure	Encryption over the wire and at rest
Established customer base	Key management/handling
Geographically distributed data centre locations	Personnel security
Certifications	Documented, mandated, and monitored the security program
Successful audits	Security policies
Financial stability	A service built with world-class data management
SLA terms and execution	Centralized management
Privacy	Range of clients and applications supported
Documented, mandated, and monitored data privacy policies	Active Directory integration
Policy on user advertising/ agreement not to mine customer data for advertising	Range of services
Practices for safeguarding confidential or sensitive information	Policies for backup and retention
Compliance with regional or local data privacy regulations	Seeding: First backup
-	Hybrid option for local recovery and fastest time to recovery

Figure 3-3: Key Features of Cloud Market

3.8 Types of Cloud “as a Service” Model

Cloud computing, or cloud as the shorthand goes, is a computing model (**Figure 3-4**) that allows one to access software, server, and storage capacity over the Internet. Instead of purchasing and maintaining these resources within an organization's servers, the organization can outsource them to the internet, gaining information and resources on demand. For the most part, Cloud is the superior alternative to the personal servers of yesteryear. They combine the accessibility and flexibility afforded by the internet, expenses far lower than any backup site and additional hardware, and the utmost effectiveness, speed, and innovation that characterizes the digital age (Cloud computing, 2015). Occasionally, a user has to download a client code, but most horsepower is borrowed from the cloud.

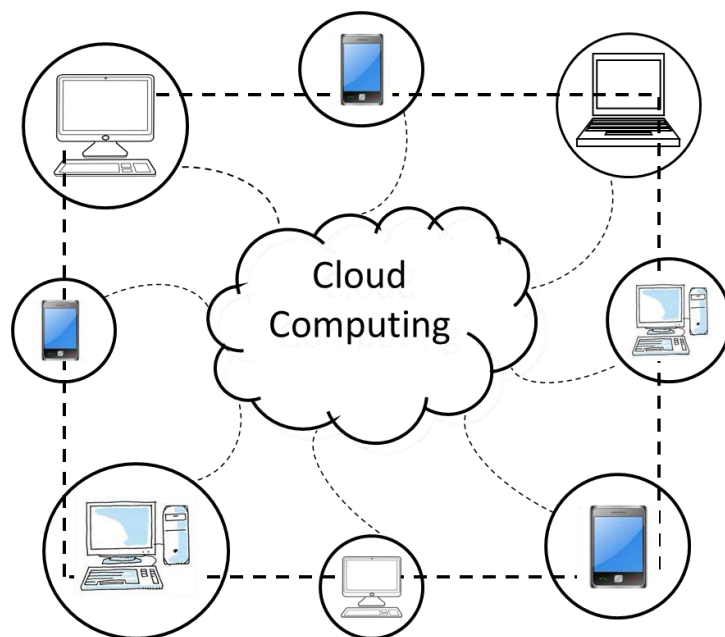


Figure 3-4: Cloud as a Service Model

3.9 Cloud Services Model

The four types of service models in the cloud (**Figure 3-5**) can be divided into:

- Software as a service (SAAS)
- Platform as a service (PAAS)
- Infrastructure as a service (IAAS)
- Recovery as a service (RaaS), which is referred to as DRaaS for disaster recovery (DR)

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

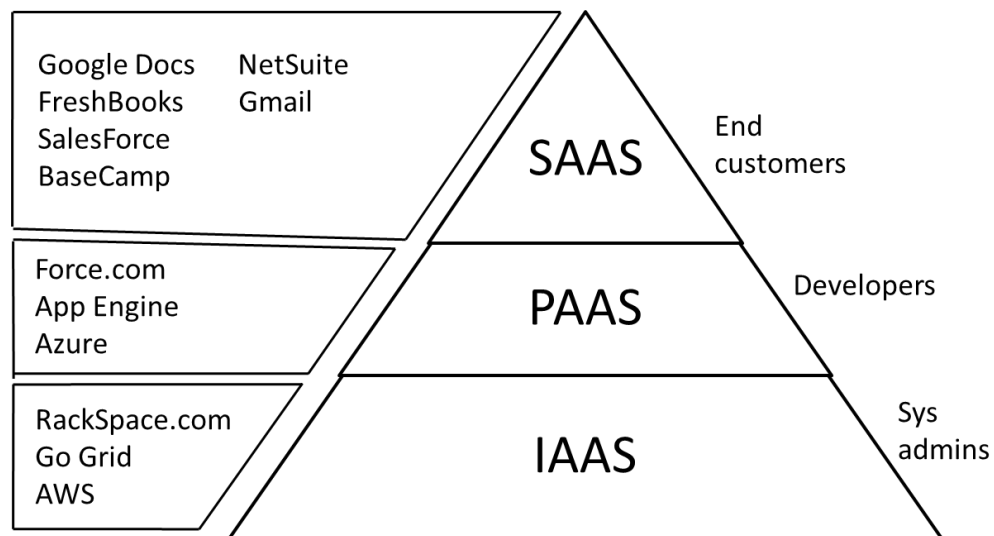


Figure 3-5: Types of Cloud “as a Service” Model

These four services are considered part of the classification of cloud computing, and they go towards End Users, who access them through devices like laptops, tablets, computers, and mobile phones.

3.9.1 Software as a Service (SAAS)

SAAS serves as a software licensing and delivery model in which software is licensed as a service over a web browser or a program interface. It is centrally hosted and is also referred to as software-on-demand. Sometimes, the software is licensed on a subscription basis. Some SaaS examples include email, CRM, Google applications, online video games, Zoho office, and even Facebook and Twitter (SaaS, 2015).

3.9.2 Platform as a Service (PAAS)

PAAS, in short, is a platform that provides a virtual platform that allows customers to run and manage internet applications without the hassle of constructing and building up their app infrastructure from scratch. It is associated with bypassing software development by using a developer's software, utilizing its assorted tools and services to create its applications. Examples include Force.com, Google app engines, Windows Azure, and Red Hat OpenShift (PaaS, 2015).

3.9.3 Infrastructure as a Service (IaaS)

IAAS is the third of the service models of cloud computing. This brand of service is also referred to as utility computing. IAAS provides resources through the cloud, usually the internet, as with the first two cloud computing services. However, what sets IAAS apart from the first two is that this service focuses on virtualized hardware and online infrastructure as a much better alternative to the bulkier physical hardware (Interoute, 2015), processing and networking, storage capacity and different computing resources.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

In addition, the user has complete control over any operating systems and deployed applications. Examples of IAAS include Amazon Web Services, Flexiscale, GoGrid, Rackspace Mosso, Servepath, and other servers and VMs.

3.9.4 Recovery as a Service (RaaS)

Relating directly to disaster recovery, DRaaS (RaaS, 2015) is the fourth cloud computing service. For DR, it will be referred to as DRaaS. Before the cloud, DR, as a subset of Business Continuity (BC), was primarily used for IT-intensive companies that operate highly sensitive critical applications. Prime examples include those in the financial industry, such as banks and stock exchanges. That, to put it, was an incorrect assumption. At the very least, every business needs to have a DR strategy in place, even if they do not commit only a token amount of resources to it. For example, consider a massive earthquake that destroys the primary office or a tsunami that does the same to the backup sites. Some countries are lucky enough to lack natural disasters, but most others are at least susceptible to fewer than one or two. Moreover, even with that considered, no country is truly immune to the possibility of a terrorist attack or even something as mundane as a fire outbreak (Progression, 2012).

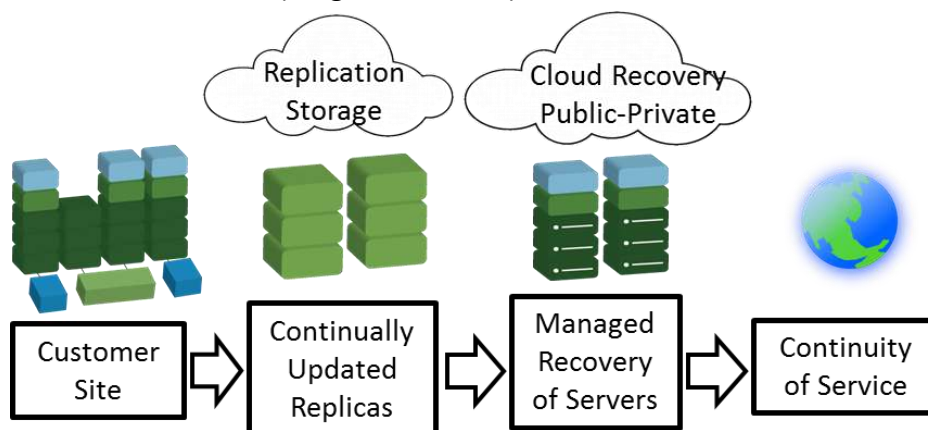


Figure 3-6: An Example of a DRaaS Deployment

Source: (Promedia, 2015)

DR is necessary. Will a business cease its services and operations simply because of an earthquake? A well-prepared business would not. The primary operations site may be decimated, but customers are still around and about. However, competent traditional DR implementation means storage and backup sites, says extra hardware and software means synchronicity between data of the primary, secondary, and, where relevant, tertiary centres. On top of that, it requires the staff to know how to respond during a disaster and be trained to do so.

It is, in a word, expensive. The costs of such DR investments discourage smaller companies from really implementing DR – until DRaaS (**Figure 3-6**) comes into the picture.

3.10 Management of “Cloud as a Service” Providers

The explanation of the many Cloud as a Service models and the organisation's involvement and the service provider is presented in **Figure 3-7** in its respective computing layers. It is important to note that the recovery of the " service type," if it is outsourced to the service provider, will be managed externally. The agreed service level agreement becomes the main component in meeting the RTP and RPO business process and applications.

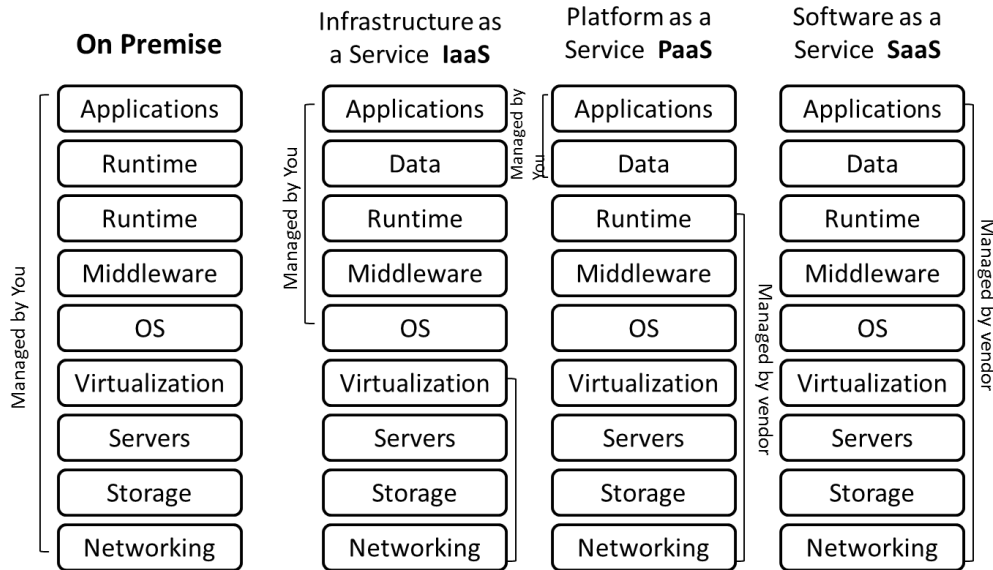


Figure 3-7: Management by Vendor as a Service

3.11 Traditional Disaster Recovery (DR)

With the introduction of cloud computing, traditional Disaster Recovery (DR) appears to have a gap (**Figure 3-8**) and poses many challenges, as shown in **Figure 3-9**. It cannot survive on its own, and from the perspective of a small business, it can often take too much out of the financial budget to run anything resembling a typical DR plan. Thanks to virtualization and the Internet, DR is a more convenient affair now. Thanks to the public cloud, DR can now be taken even one step further, ignoring the bulk excesses of a physical backup site and the extra hardware it would entail (Barret, 2014). Disaster Recovery as a service, or DRaaS as a shorthand, is the key to DR in the present and, as far as we know, shortly to come.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

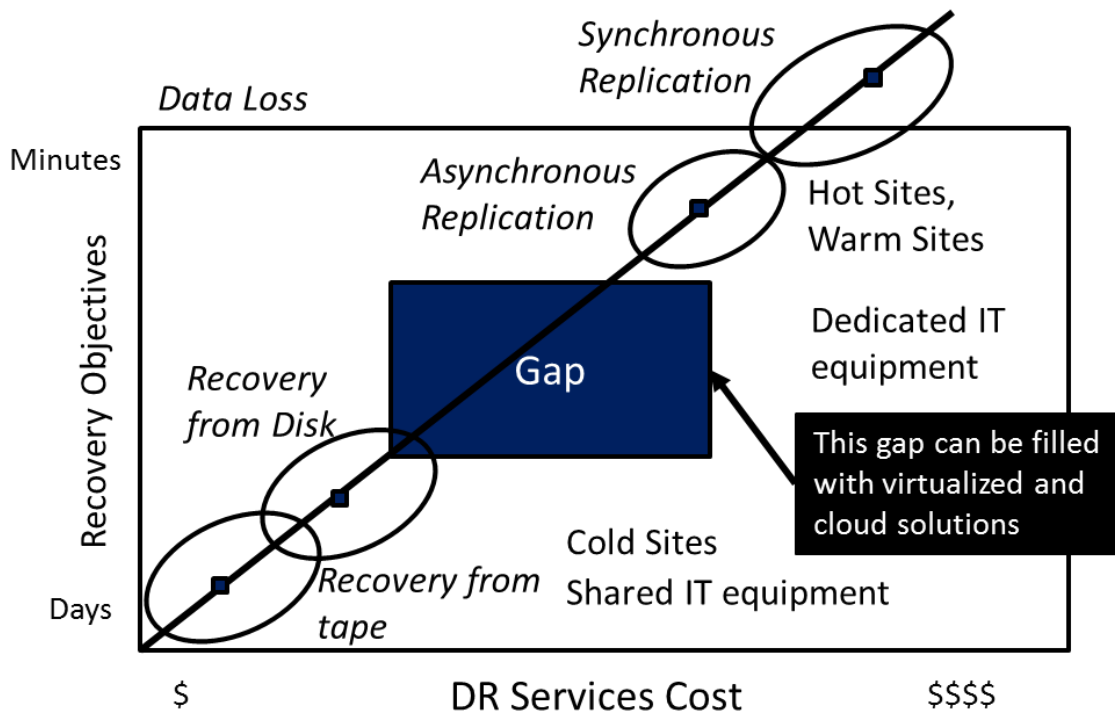


Figure 3-8: The Gap in Traditional DR Services Source: (Gibilisco, 2014a)

Disaster Recovery is hardly a new concept in the IT world. Still, while prolific and steadily growing in popularity, the transition to the cloud seems to elude some older, more traditional businesses. Between 2012 and 2016, one-third of organizations are looking for newer, more effective methods to replace their current ones specifically because of issues like cost, complexity or capability (Latulippe, 2015). Additionally, DraaS is, as an industry, expected to grow and expand at a rapid rate over the next half-decade, illustrating its massive potential. Spending on it is predicted to rise to \$1.2 billion (£766 million) by 2017. In fact, by the estimates of experts, the industry could very well be worth \$5.7 billion (£3.4 billion) by 2018 (Pudwell, 2015).

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

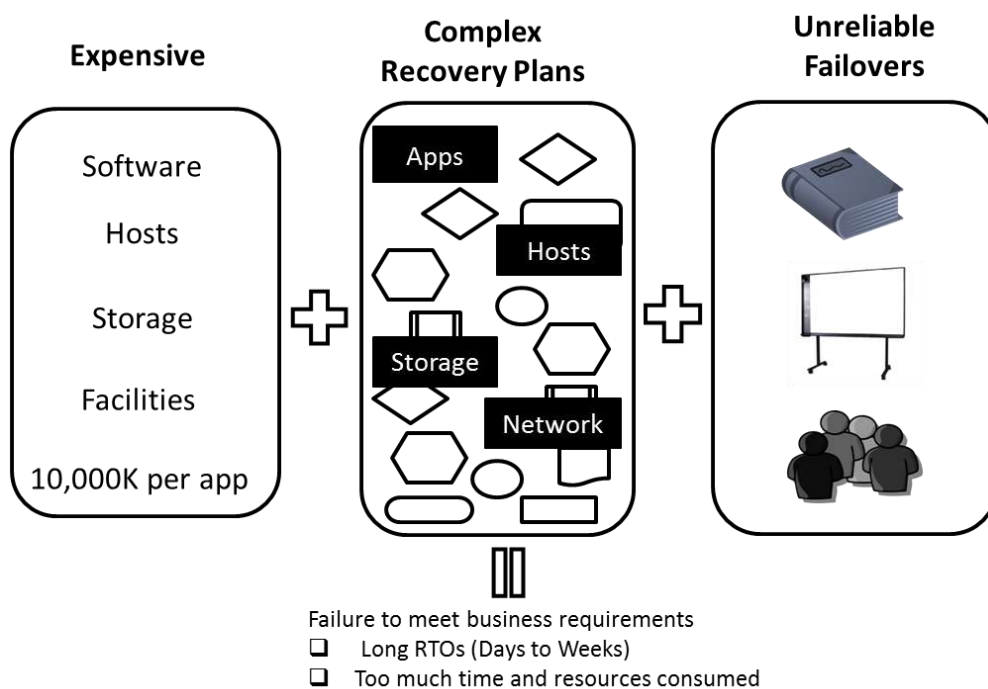


Figure 3-9: Challenges of Traditional DR Source: (Croteau & Evans, 2014)

3.12 Disaster Recovery as a Service

However, what is DraaS? Is it simply offloading DR processes to a cloud, or is it something far more specialized than that? DRaaS is ‘the replication and hosting of physical or virtual servers by a third-party to provide failover in a man-made or natural catastrophe’ (Gibilisco, 2014b).

There is a significant distinction between traditional cloud backup and the cloud disaster recovery that is DRaaS. While, on the surface, both involve backing up data, the latter is often more specialized to ensure that data survives whatever disaster may befall you and your organization (De Stefano & Onoprijenko, 2015). DraaS provides that a standard cloud backup does not necessarily do a virtual server, adequate infrastructure, and knowledge and expertise to operate and navigate the virtual environment and software applications.

3.12.1 Advantages of DRaaS

Of course, with these added benefits come extra costs, both financial and otherwise. DraaS, besides the expenses required for setting up the corresponding server and getting the infrastructure up, it is far more labour-intensive than a simple cloud backup solution. An organization’s choice of what level of protection should be adopted would be decided based on an organization’s recovery time objective (RTO). If the RTO is flexible and, for example, over 24 hours, a cloud backup would suffice to tackle the problem. Cloud disaster recovery is recommended if the RTO is rigid and less than 24 hours.

A thing to note: DraaS is not a solution to be brought out only for emergencies. A problem that spans both traditional DR and DraaS is the simple fact that many organizations still

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

regard DR as a reaction solution to a problem rather than a proactive one. DR's intention as a 365/24/7 failsafe for your organization serves to guard your data, and it should not serve as some last resort to be whipped out when trouble comes calling. The threat of business disruption is a forever-present looming threat, and vigilance is needed to catch it before it falls (De Stefano & Johnson, 2015).

3.13 DRaaS Versus Traditional DR

What are the advantages of DaaS when matched against traditional DR? What can DR on the cloud give that the old methods fail to provide? Price, of course, is the most immediate and obvious talking point between the two methods. Traditional DR demands exorbitant prices for the most responsive IT services, including a complete duplication of the hardware in the main site, the costs of a backup site, tape devices and media, and the necessary software to ensure synchronous replication of the data. Additionally, complex licensing paths may also force the use of specialists to decipher it, incurring even more expenses (Paul, 2015). Cloud DR? Cloud DR has little of that. Maintenance expenses fall under the purview of the service provider rather than the receiver. Organizations only have to pay for the resources they consume rather than spend money on needlessly maintaining systems that could be used only once per year. (De Stefano & Casey, 2015). It is a far superior viable option and highly elastic; the ability to offload everything to the cloud makes it much more manageable.

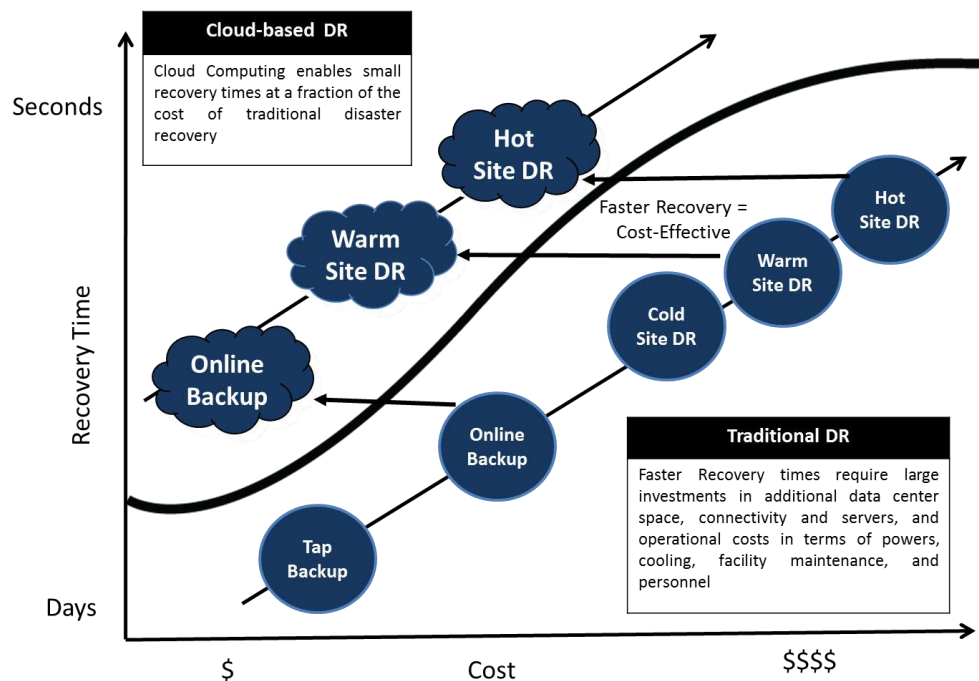


Figure 3-10: DRaaS versus Traditional DR

4 Project Management



“Plan for what is difficult while it is easy. By deep knowledge of principle, one can change disturbance into order, change danger into safety, change destruction into survival, change calamity into a fortune.”

Sun Tzu

4.1 What is Project Management?

This book starts with the assumption of the appointment of the Executive Sponsor and the Organization DR Coordinator. But unfortunately, the appointment process usually proves a long-drawn affair as it is political and highly dependent on the organisation's motivation.

The first step in implementing DR is to set up the required Executive Management structure to support the process. It is followed by creating the DR team and the appointment of the Team Leaders for the several groups and team members, usually presented in a presentation and project charter to be approved by Executive Management.

Next, it confirms the business units and their functions to be included within the scope of the DR Planning project. Finally, each party's roles and responsibilities during the project ensure the practical completion of task assignments and time goals set at later stages.

Obtain the commitment of heads of business units and their staff members and involve them in the DR planning process. Identify and mobilize the business unit's resources and begin the information-gathering process.

After completing the DR Planning process, the final product will be a DR Plan.

4.2 Deliverables

The final deliverables (Goh, 2008c) expected by the Executive Management are:

- A project proposal or charter to Executive Management that includes the definition, scope, objective, roles and responsibilities, and budget

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- A project works plan
- A project reporting mechanism

4.3 What Does Project Management Entail?

The entire project planning process (*may not be in the order of implementation*) involves the following steps:

- Step 1: Establish the Need for DR Planning
- Step 2: Research Your Work
- Step 3: Develop a Framework
- Step 4: Develop Corporate DR Planning Policy
- Step 5: Define the Scope, Objectives, and Assumptions
- Step 6: Manage the DR Planning process
- Step 7: Establish a Steering Committee and Project Planning Team
- Step 8: Develop an Action Plan and Schedule
- Step 9: Establish a Budget
- Step 10: Obtain Commitment and Approval
- Step 11: Manage Deadlines and Milestones
- Step 12: Build and Maintain Teamwork

4.4 Step 1: Establish the Need for DR Planning

DR Planning is about being prepared to rebuild your business organization after a disaster to provide continuity in customer service at a minimum acceptable level, particularly in providing information and communication systems.

Business organizations are driven by business processes, which are chains of activities executed across business units. Each organization consists of an integration of business processes, the participants in these processes, and the infrastructure and resources supporting these business processes. Computer systems and networks play a critical role in linking the organization, internally between its various business units and externally, with customers and suppliers. The loss of this capability has dire consequences for the organization.

It would be helpful to refer to **Appendix M for a list of Frequently Asked Questions** for possible questions you may ask as an Organization DR Coordinator.

4.5 Step 2: Research Your Work

The first steps in creating a DR plan are understanding what the Executive Management in your organization expects in this plan and assembling the knowledge to deliver a plan that meets their expectations.

Whether you have some BCP or DR Planning background or are a newcomer, many websites will quickly get you up to speed.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Several sites worth mentioning are the Disaster Recovery Journal and the Continuity Central sites, as they contain articles explicitly aimed at helping Organization DR Coordinator and Organization BCM Coordinator. They want to learn or brush up on the fundamental principles. If this is a new professional area for you, spending a few hours reading those articles should help make you much more knowledgeable quickly.

There also are many organizations, ranging from international to local, where you can network with your peers. Look for their websites, including chat rooms, using search engines with keywords like business continuity or DR. These knowledge base sites contain many articles, profiles and case histories of plans, and BCP/DR Planning products, services, and resources. Another critical requirement is to standardize your glossary of DR terms within the organization before starting the DR planning project. A sample of the glossary for DR can be found in **Appendix N**.

4.6 Step 3: Develop Framework

The start of framework development begins with a clearly defined strategic vision for Disaster Recovery Planning. This framework should already exist if the organization has a business continuity management team. DR Planning will form part of this overarching framework and be guided by its policies, standards and guidelines. If such a framework does not exist, the team should endeavour to develop one.

Here is a simplified approach to developing the framework.

4.7 Step 4: Develop Corporate DR Planning Policy

The development of the DR Planning Framework is immediately followed by a policy directive stating their commitment to DR Planning in general and this project in particular. If they agree to this request, the DR Planning project will have gained a lot of credibilities. On the other hand, if they would disagree, you will, at least, have been forewarned that the Executive Management's support for the DR Planning project is lukewarm at best and that you should proceed cautiously.

4.8 Step 5: Define Scope, Objectives, and Assumptions

4.8.1 Design Clear Objectives

One measurement of the Organization DR Coordinator's success will be whether the final product satisfies the Executive Management's requirements.

In much the same way as the Organization DR Coordinator needs to know what is expected of them, there must be agreement as to what precisely the DR Planning implementation will achieve the project's desired outcome.



One of the important outcomes is to understand DR's business goals on DR. Though this is initial and brief, it will provide good directions on what functional areas to recover and what length of time and data loss is acceptable for recovery.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

4.8.2 Develop Clear Scope

The Organization DR Coordinator needs to consider how much the operations will be covered. For example, whether it will be a phased recovery and whether PCs should be included if you are in a minicomputer or mainframe environment. It should also consider whether the organization expects "immediate" recovery of all applications and business functions to the whole operating level or only the critical applications, business functions, or something in between.

While defining the scope of the DR Planning project, the planning team will need to identify:

- Ane entire organization or just its specific business unit.
- The nature and impact of the disaster, such as the worst-case scenario.
- The resources required for the project.

4.8.3 Document Limitations and Assumptions

Identifying the "IS" and "IS NOT" in a standard project management exercise is crucial. Then, you can ensure that there is no confusion or disagreement about what will or will not be included within the scope of the DR Planning project. If, for example, the DR Planning project will not address multiple site disasters or the loss of key personnel, document this as a limitation that will be treated in a subsequent DR Planning project.

Here are some examples of assumptions:

- Staff are denied access to the office building for a sustained period of seven calendar days.
- Extend planning to commence on day two or three if the crisis exceeds seven calendar days.
- Address only critical business functions and not daily operational contingencies.
- Only critical business functions will be prioritised during the seven calendar days.
- No more than one country will be affected concurrently by the same disaster.
- Disaster occurs at the most vulnerable time for each business function.
- DR Plan for an IT functional unit is already in place and tested.
- Alternate staff and replacement equipment are available within planned timeframes.

It is imperative that these objectives, scope, limitations, and assumptions be in writing and signed off by the Executive Management. Any subsequent changes must also be in writing, and the timeframe and resource allocations must be amended.

4.9 Step 6: Manage the DR Planning Process

4.9.1 Break the Project into Phases

A DR Planning project will remain a major undertaking even with a limited scope. The DR Planning project should be broken down into discrete phases to keep it manageable.

The DR Planning process or methodology provides an essential overview of such phases. Like another planning process, it offers a framework for requirements, effort, and deliverables, leading into the next "phase" of an endlessly repeating cycle. In real life, many of these phases may be conducted simultaneously. While this process does provide visual clues as to the amount of time and changing emphasis within a phase, these are for reference and do not represent an absolute percentage of the time. The DR Planning process, as explained earlier, includes the following phases:

- Project Management
- Risk Analysis and Review
- Business Impact Analysis
- DR Strategy
- Plan Development
- Testing and Exercising
- Program Management



4.9.2 DR Project Plan

A DR project plan should be established to manage the tasks, deadlines, and deliverables. The significant steps of the typical DR project plan are shown below. The description of each phase and its major activities are further elaborated in **Appendix G: DR Planning Project - Major Activities / Milestones**.

4.10 Step 7: Establish a Steering Committee and Project Planning Team

Before starting the DR Planning project, the organization must identify the key personnel. Essential personnel includes the formation of a DR steering committee and bringing together the DR Planning team.

4.10.1 DR Steering Committee

Usually, the Executive Management is the sponsor of the DR Planning project. In addition, the committee should appoint senior members of the organization as members of the DR Steering Committee. This steering committee has executive oversight and supervision over the DR project team. This DR Steering Committee meets once or twice monthly

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

during the initial project. Once the DR planning project is completed, they must meet twice to four times yearly.

4.10.2 DR Project Team

The Organization DR Coordinator leading the DR project team should include the following members (Organization DR Coordinators) of the organization:

- Executive Management.
- IT Staff Members.
- Members of the Business Unit.
- Members of the Support Unit.

IT Business Unit/ Function	Responsibility (Assist businesses with their IT requirement)
Information Technology	Switch to backup systems.
Voice and Telecommunications	Switch to backup voice and telecommunications systems.
Network Management	Reroute to alternate networks.

Figure 4-1: Responsibility in DR Planning (IT Staff)

Business Unit/ Function	Responsibility (Develop Procedures to)
Facilities Management	Maintain damaged facilities, acquire new or temporary facilities and provide logistical support to move staff and equipment.
Human Resources	Communicate with employees during a disaster.
Legal Counsel	Review and advise all regulatory and contractual requirements for DR.
Mailroom	Operate in the alternate mail room.
Manufacturing and Production	Run alternate manufacturing processes or at alternate locations.
Marketing	Determine how to leverage DR Planning as a marketing tool.
Research and Development	Conduct research and development processes at alternate locations.
Sales	Conduct sales processes at alternate locations.
Shipping and Receiving	Continue to provide shipping and receiving support and facilities.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Business Unit/ Function	Responsibility (Develop Procedures to)
Public Relations	Facilitate awareness programs and Communicate with external entities during a disaster.

Figure 4-2: Responsibility in DR Planning (Business Unit)

Type of Staff	Technology Support Areas
Network management staff	Wide area network and Local area access
	E-mail access
	Data backup and restoring data
	Access for telecommuters and mobile workers
Data centre operations staff	Ensure the functioning of enterprise applications and business unit-specific applications.
IT security staff	Maintenance of systems security
E-commerce staff	Functioning e-commerce applications, including Web servers, EDI applications, and supply-chain systems

Figure 4-3: Areas in which IT and Networking Management assist DR Planning Team

4.10.3 Clear Terms of Reference (TOR)

The Terms of Reference for a DR Planning project can be likened to the syllabus for a course of study. Without an agreed syllabus, you will not know what you will be examined for, and the chance of passing is negligible. DR Planning project management is like leading up to an exam and the exam itself. You need to know what is expected of you, what specific authority you have, and what the limits are. All too often, an organization will take a position, which has been ill-defined, if at all, and this is the first step to possible failure.

4.11 Step 8: Develop an Action Plan and Schedule

4.11.1 Create a Schedule

It is challenging to schedule and estimate the time needed for a DR Planning project. The issues are that there are never enough people and never enough time. So how do you know you have identified all the work? This section will guide you to determine the most important tasks to be taken care of and the obstacles to watch for when establishing the DR Planning project schedules and estimating individual task duration.

4.11.2 Get Agreement on Dates

When assigning tasks to team members, it is unwise to state, "I need this task completed by such-and-such a date." Without input into the scheduling process, the team member may not accept accountability for meeting the target. Instead, ask, "How soon can you complete this task?" Negotiate if necessary, but be sure to get an agreement and hold the team member accountable for meeting the agreed-upon date.

4.12 Step 9: Establish a Budget

People tend not to take something seriously, especially DR Planning, unless it has a budget. The Organization DR Coordinator must build a budget and approve it early. There is no rule of thumb for the cost of developing and implementing a DR Plan. I recommend that the budget estimate you present to the Executive Management should be built on the careful definition and solid research.

Arriving at that number requires the team to define resources and financial requirements, verify the validity, and negotiate each with the Executive Management. In Europe and North America, one factor favouring implementing a DR Planning program is that insurance companies now provide discounts for organizations that maintain effective BCP and DR Planning programs. They eventually may mandate the testing of DR procedures before they issue loss of business insurance due to a business or computer outage. Plug into your budget and estimate the savings or potential savings in insurance. Suppose the corporate insurance is not applicable in your country when you determine the budget for a DR Plan. In that case, you should consider the resources needed to write the DR Plan, test the plan, heighten the Executive Management's awareness of the critical business function or application systems already in place and assess the backup capabilities required to recover within the allotted time.

4.13 Step 10: Obtain Commitment and Approval

The Organization DR Coordinator should insist on and ensure that formal approval for the DR Planning project is obtained. As part of the approval, the Organization DR Coordinator will need to prepare a written DR Planning project proposal (or charter), including estimated costs and staffing requirements, and request that it be signed by the Executive Management in all affected areas. It is imperative not to rely upon verbal approval alone.

4.14 Step 11: Manage Deadlines and Milestones

4.14.1 Issue Recommendations After Each Phase

Breaking a DR Planning project into phases and helping keep the project manageable provides an opportunity to gain Executive Management commitment incrementally. After completing one phase, recommendations can be issued on proceeding with the next phase. Since the ability to produce results will already have been demonstrated, the Executive Management should be predisposed to endorse the recommendations. As

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

each phase builds upon another, the Executive Management's comfort level in making DR Planning project commitments will increase.

4.15 Step 12: Build and Maintain Teamwork

4.15.1 Communicate and Participate

The Organization DR Coordinator should conduct communication at all levels. Assertive communication is one of the strategies to build a winning team and should be implemented whenever possible.

- Get out of your office and talk to people.
- Make contacts.
- Use the experience of others.
- Develop a network of allies and know your opposition.
- Develop your credibility by giving supervisors and peers something they can use.
- Emphasize survivability and sustainability of organization and safety and continued the employment of personnel.
- The key to project management success is choosing the right people, equipping, encouraging, and managing effectively.
- Recruit the most qualified people – do not take a body to fill a position
- Involve first-level management in the project, and then they will involve their staff
- Facilitate and coordinate with managers of team members who do not report to you
- Motivate team members to contribute their best
- Do not over-supervise team progress
- Set expectations of success
- Resolve technical disagreements early
- Facilitate team growth: Form, Storm, Norm, and Perform
- The team sets its ground rules and lives by them
- Instil a sense of mission
- Help team members see the big picture

5 A Management Proposal for Implementing the DR Plan

5.1 Overview

Executive Management's recognition and support are key factors in successfully implementing a DR plan. Because the process of developing the DR Plan is very resource-intensive, it needs to:

- Identify the related parties in the organization and involve them in analyzing, preparing and documenting risk and recovery processes.
- Seek sources of funds to procure DR equipment, software, services, awareness and training programs.
- Provision for resources to continuously maintain, update and test the DR plan to keep it current with the IT operating environment.

Often, some Executive Management questions the need to invest resources and funds into developing and maintaining the DR function as it is not a revenue-generating activity. As an Organization's DR Coordinator, there is a need to provide a well-thought strategy by collecting enough statistics and information to convince the Executive Management to allocate the resources to support the development and subsequent maintenance of the DR Plan.

5.2 Management Proposal Format

These are the important items to be included in a management proposal.

5.2.1 Objective and Scope

Like any other management proposal paper, a clear objective and scope must be specified clearly so that the Executive Management can understand what they are endorsing. In addition, the clarity in this section seeks the commitment of resources, budget, and time to develop the DR Plan for the organization.

5.2.2 Historical Facts

Research and studies must be carefully done to ensure sufficient information to establish your business case for initiating a DR planning project for the organization. Some of the significant historical facts that you should research include:

- Past disruptions within the organization have caused considerable losses or inconvenience.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- News and figures on disaster events may have happened in the exact geographical location of your organization or areas where your organization has a presence.
- Financial/business losses due to disaster events for the same industry.
- Financial/business losses due to disaster events for business partners.

5.2.3 Mandatory Requirements

One strong justification is highlighting any mandatory requirements such as statutory, contractual, industrial, or military. Also, highlight any formal service level agreements your organization has with its business partners, customers or government authorities with an agreed tolerable unavailability window. Otherwise, substantial penalties may have to be paid to these external parties.

5.2.4 In-house or External Approach

This section highlights the approach to carrying out the DR project planning process. For example, does the organization need to engage a DR consultant to assist in managing the entire DR Plan development cycle, or is the organisation capable of doing it themselves? The list of the pros and cons of the proposed approach is elaborated.

5.2.5 Resources

Estimate the following resources that are required to develop the DR Plan:

- The workforce needed to develop, test, verify and maintain the DR Plan.
- The budget for engaging DR consultants, DR services, hardware and software, and training of the DR teams and general users.

5.2.6 Project Schedule and Key Milestones

Provide an overview of the complete project development schedule with an indication of significant milestones such as completion of risk analysis, business impact analysis, development of DR strategy, etc. Also, indicate the management reporting structure and the timeline for reporting project development progress to the Executive Management.

5.2.7 Budget

The budget is the source of funding for the DR planning project.

5.2.8 Key Responsibilities

The responsibility of each business unit and function should be published to ensure that all staff participating in the DR Planning project clearly understand their roles and responsibilities. A sample can be found in **Figures 3-1 and 3-2**.

5.2.9 Risks and Exposures

One has to consider the likelihood of exposure to events with the potential to cause considerable disruption to your IT operations. Critical services and infrastructure must be carefully considered, such as power supply sources, telecommunication linkages, cabling risers, hardware, and software. For example, suppose your organization shares a typical telecommunication cable riser with other tenants in a building. In that case, the potential risk of someone accidentally cutting off your telecom cable is relatively higher than if your organization had exclusive use of a riser. Estimate the time you would need to recover telecommunications if the cable is accidentally cut and what the loss would be to your organization during the outage period. The estimates are usually obtainable through the various business unit owners who use your IT systems or infrastructure to support their business operations.



This section may not be available at the start of a new DR planning project and may be excluded from the proposal. This section aims to give your Executive Management a feel of the IT operational risks your organization is facing and the potential damages the business operation is liable for.

5.2.10 Overview of Preliminary Strategy

Present an overview of the measures your organization can take to prevent, minimize and recover from disaster events that may impact its business operations. Then, compare the pros and cons of each measure before putting forward your recommended strategy.



This section may not be available at the start of a new DR Planning project and may be excluded from the proposal.

5.3 Quick Answers to Common Attitudes and Objections

Like all other management project proposals, there are always agreements and disagreements among the Executive Management. However, they must be comfortable with why the organization is committing resources and spending money on projects that may not be seen as profit-generating. So, as an Organization DR Coordinator, you must be prepared to convince your Executive Management of the need for a DR Plan. Here are some common objections or attitudes that the Executive Management may have and how they can be addressed from a DR practitioner's point of view.

5.3.1 "Is it a problem?"

The Executive Management may decide against a DR Plan because the impact is negligible and the Executive Management is willing to take the risk. Alternatively, the Organization DR Coordinator has not been clear on the potential business loss should a disaster affect the organization's IT support services.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

5.3.2 “We have no time for a DR Planning project.”

Lack of time may happen unless you illustrate the importance of a DR Plan well. Give examples of organizations significantly suffering from disaster events because they did not have DR processes. Substantial statistics, news and third-party reports will help.

5.3.3 “Our insurance will cover the damage; we do not need a DR Plan.”

Insurance only covers the purchase cost of hardware, software and sometimes a certain amount of data. It does not assure you of IT recovery and business continuity.

5.3.4 “You are spending money to satisfy the auditor.”

If this is a fact, your organization needs a DR Plan because even the Auditor has said so. However, highlight to your Executive Management that a DR Plan should not be developed to satisfy the auditors.

The key objective is to ensure that the critical part of the business can continue in times of disaster unless your Executive Management is willing to absorb all risks of business failure. Therefore, having a DR Plan goes beyond satisfying the auditor. It is necessary if your organization wishes to help your customers, shareholders, the authorities, and your corporate governance.

A DR Plan should form part of your organization's overall business continuity strategy. You need to bring forward also the importance of up-keeping the DR Plan as frequent changes in the business environment impact the supporting IT infrastructure and services. A DR Plan that is not constantly updated is another historical document with no value during a disaster.

5.3.5 “We can still function without IT services.”

A business impact analysis should be conducted to ascertain that business operations do not depend on IT support services. Provide statistics and workflow charts that indicate all the dependencies on IT services to the Executive Management.

5.3.6 “The DR Plan is too expensive.”

Have you gotten enough statistics to substantiate your cost estimates? Then, do careful research with DR Service providers for the scope of services required, seek realistic expectations on RTO from business systems owners and analyze the likelihood of the risks occurring.

Suppose there is a budget problem, and you are confident that your initial research is accurate and complete. In that case, you may seek the Executive Management's approval to reduce the scope of their recovery expectations.

5.4 Conclusion

Making the Executive Management see the importance of the DR Plan to the organization is challenging but rewarding. This is because the Organization DR Coordinator has added value to the organization by ensuring its ability to quickly respond to and recover from potential disasters, safeguarding the shareholders' interests, investments, and jobs.

6 Risk Analysis and Review



"DR Planning deals with preparing for Moreover, avoiding events that you hoped will never happen."

Goh, Moh-Heng

6.1 Overview

Today, most businesses depend heavily on technology and automated IT systems to support their day-to-day functions. Thus, disrupting the technology or systems will cause severe financial loss and threaten the business's survival. For example, even if the disruption were to last for just a couple of hours to the primary computer system at the stock exchange, the entire stock market would be at a standstill. Can you imagine what the result will be?

Identifying potential disasters, analysing their impact on your business, and developing countermeasures against them quickly and effectively is the key to business survivability in this technological age. Moreover, the technical term for this process is called Risk Management.

In this chapter, we will focus on the following three keys processes of the Risk Analysis and Review phase :

- Risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.
- Risk assessment involves evaluating existing security and controls and assessing their adequacy to the potential threats to the organization.
- Risk treatment involves identifying and implementing measures that reduce, mitigate, transfer or remove the potential threats to the organization.

So that you can keep your management aware of potential disasters, you can equip yourself with the ability to develop a plan to minimize disruptions to your mission-critical functions and thereby increase your organization's capability to recover operations quickly and successfully should a disaster happen.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

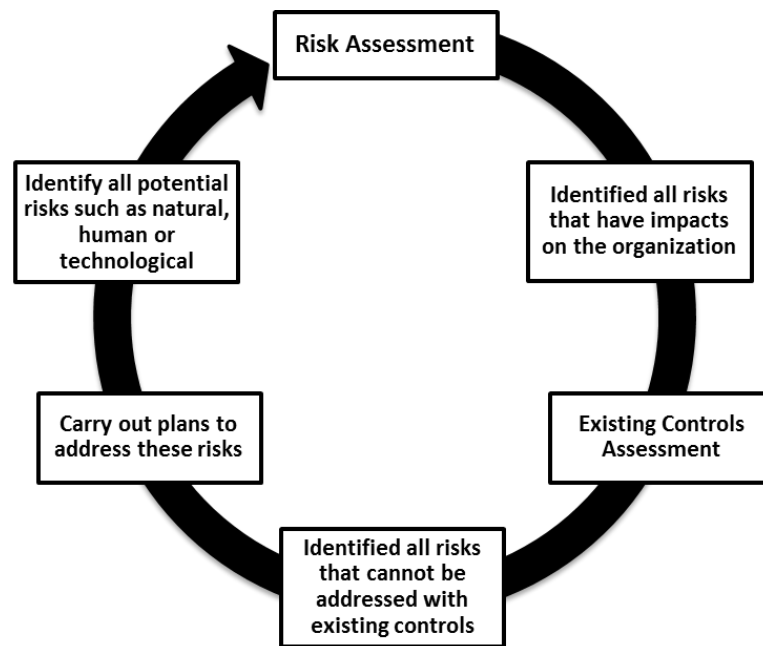


Figure 6-1: A typical Risk Assessment Workflow

6.2 Deliverables

After the risk analysis and review process is completed, the final output of this process is a report that includes the following:

- A prioritized list of the critical assets supporting critical functions and applications.
- The prioritized and description of the risks.
- An evaluation of the existing controls and areas where controls are not implemented.
- Recommendations for enhancement of the existing controls and new controls.

6.3 Risk Analysis

Firstly, we would like to reiterate the goals of the DR Plan. It ensures the continuity of all IT systems to support business operations in any disastrous situation or event.

The Risk Analysis process starts with identifying and measuring the likelihood of all potential risks that can happen and their impact on the organization.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**



Figure 6-2: Risk Assessment Computation

When we identify the potential risks, we should not be limited by our current operational constraints. We should be open and list all possibilities, for example, geographic location, proximity to significant sources of power, bodies of water and airports, degree of accessibility to facilities within the organization, history of local utility companies in providing uninterrupted services, history of the area's susceptibility to natural threats, proximity to significant man-made hazards, such as petrol stations, power plants and train stations, etc.

In general, all potential risks can be grouped into the following four categories:

- Natural**
Hurricane, tornado, flood, earthquake, storm, and fire
- Man-made**
Operator error, sabotage, terrorism, war, arson, and malicious code
- Business**
Power outage, Labour disputes, key employee turnover, and loss of transportation
- Technological**
Equipment failure, software error, telecommunications network outage and electric power failure

It may be helpful to note that threats categorized under business or technological may be considered Man-made threats. Not all risks are present concerning a given IT business unit. For example, depending on its location, a system may have no risk of damage by the hurricane but a reasonably high risk from the effects due to a tornado. A risk assessment is required to determine the specific risks to a system effectively. Use **Figure 6-3, List of Threats**, to identify the threats that could occur to your organisation.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

List Of Threats (C= Country / O = Organisation)								
Denial Of Access	Occurrence		Unavailability Of People	Occurrence		Equipment and It-Related Disruption	Occurrence	
	C	O		C	O		C	O
Flood/ Flash Flood			Labour Dispute/ Strike			IT Failure (i.e. Hardware, Software)		
Lightning			Infectious Disease/ Pandemic			Network Failure (i.e. Local and Wide Networks)		
Tropical Storm			Workplace Safety			Facilities and Equipment Failure (i.e. Air-con, Lift, Transformer, HVAC, UPS, Backup Generator)		
Cyclone			Workplace Violence			Telecommunications Failure (phone line)		
Monsoon Rain			Mishandling of Hazardous Materials			Disruption Of the Supply Chain	Occurrence	
Heat Wave			Haze				C	O
Storm			Loss of Key Appointment Holders			Loss of Specialized Vendor/ Partner/ Supplier		
Earthquake Tremors						Regulatory or Legal Violation		

Figure 6-3 List of Threats

6.4 Risk Assessment

Risk assessment is critical because it enables the person responsible for DR to focus risk management efforts and resources on identified risks in a prioritized manner. In addition, assessing the impact and consequences resulting from the loss of critical information and IT services is vital. This will enable the organization to identify and select effective and efficient recovery strategies, or prevention controls, to protect the organization's critical IT operations and services; or recover these operations and services in the shortest possible time in a disaster.

A thorough risk assessment will identify all potential risks and determine the probability of the risk occurring. Traditionally, fire poses the greatest threat to an organization. However, with the recent changes in political and economic trends and development like terrorist bomb attacks, war, and worldwide (COVID-19) or region-wide epidemics (like Severe Acute Respiratory Syndrome, or SARS), disaster scenarios have to be updated to cater to such threats. These threats cover denial of access to facilities and the loss of critical human resources or their inability to function effectively. Thus, the DR Plan had to provide for the worst-case situation, such as the destruction of the main building and

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

restricted or no access to critical human resources. Usually, the list of potential risks can be filtered to a list of probably identified risks, including those with a measurable likelihood.

To make the risk assessment realistic and practical, we should assess the potential for each type of risk at a business unit level rather than at the organization level. This is because some business units may greatly depend on some computer systems while others may not.

An excellent technique to carry out a risk assessment is to use a rating system that gives a solid visual feel of the impact of the risk on the organization's business. The first step is to draw up a risk rating, such as **Figure 6-4 Descriptor for Risk Impact and Impact Area**. Then assign a numeric rating to each of the potential risks in **Figure 6-5: Threats and Impact Area Assessment** that have been identified to determine their impact on organizational operations.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Risk Impact	Descriptor	Impact Area						
		Financial	Processes (Business Operations)	Legal and Regulatory	Reputation and Image	Social Responsibility	People	Assets / ICT Systems / Information
1	Very Low	Financial loss (i.e. Property/assets loss or damage, business loss, penalties) amounting to less than US\$1mil	Critical processes are unavailable for a very short period, causing negligible negative impact on the organisation's business operations and/or ability to fulfill MBCO.	Negligible impact on ability to fulfill contractual and/or statutory obligations.	Negligible or limited adverse impact on reputation and image.	Negligible impact on ability to fulfil social responsibility.	No injury, minor discomfort or nuisance e.g. odor	Critical assets/systems/information are unavailable for a very short time period, causing negligible negative impact on organisation's business operations and/or ability to fulfil MBCO.
2	Low	F Financial loss (i.e. Property/assets loss or damage, business loss, penalties) amounting to less than US\$5mil	Critical processes are unavailable for a short period, causing negligible negative impact on the organisation's business operations and/or ability to fulfill MBCO.	Minor impact on ability to fulfill contractual and/or statutory obligations.	Minor negative impact on reputation. Some adverse impact limited to organisation's stakeholders.	Minor impact on ability to fulfill social responsibility.	Minor injury e.g. cuts and bruises requiring outpatient treatment; on-site release immediately contained.	Critical assets/systems/information are unavailable for a short time period, causing negligible negative impact on organisation's business operations and/or ability to fulfil MBCO.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Risk Impact	Descriptor	Impact Area						
		Financial	Processes (Business Operations)	Legal and Regulatory	Reputation and Image	Social Responsibility	People	Assets / ICT Systems / Information
3	Medium	Financial loss amounting between US\$5mil to US\$50mil	Critical processes are unavailable for a moderate time period, causing partial negative impact on organisation's business operations and/or ability to fulfill MBCO.	Warning, fines and/or regulatory investigations by external agencies.	Moderate negative impact on reputation. Negative impact on stakeholders' confidence and/or negative publicity on various forums.	Moderate impact on ability to fulfill social responsibility.	Medical treatment required; on-site release contained with outside assistance.	Critical assets/systems/information are unavailable for a moderate time period, causing partial negative impact on organisation's business operations and/or ability to fulfill MBCO.
4	High	Financial loss amounting between US\$50mil to US\$100mil	Critical processes are unavailable a long time period, causing significant negative impact on organisation's business operations and/or ability to fulfill MBCO.	Lawsuit for damages or termination of contract	Significant negative publicity and damage to reputation. Possible adverse local media coverage.	Significant impact on ability to fulfill social responsibility.	Extensive injuries, off-site release with no detrimental effects.	Critical assets/systems/information are unavailable a long time period, causing significant negative impact on organisation's business operations and/or ability to fulfill MBCO.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Risk Impact	Descriptor	Impact Area						
		Financial	Processes (Business Operations)	Legal and Regulatory	Reputation and Image	Social Responsibility	People	Assets / ICT Systems / Information
5	Very High	Financial loss amounting equal to or greater than US\$100mil	Critical processes are unavailable for an extended period, causing severe and irreversible negative impacts on the organisation's business operations and total failure to fulfill MBCO.	Multiple lawsuits for damages or termination of the contract, possible leading to termination of operations.	Catastrophic negative publicity and damage to reputation. Adverse local media coverage and/or international media coverage.	Severely unable to fulfill social responsibility.	Fatalities, toxic release off-site with detrimental effect.	Critical assets/systems/information are unavailable a extended time period, causing severe and irreversible negative impact on organisation's business operations and/or total failure to fulfill MBCO.

Figure 6-4 Descriptor for Risk Impact and Impact Area

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Threat	Impact Area							Highest Risk Impact (Numeric)
	Financial	Process (Business Operations)	Legal and Regulatory	Reputation and Image	Social Responsibility	People	Assets / ICT Systems / Information	
(2-a)	(2-b-1)	(2-b-2)	(2-b-3)	(2-b-4)	(2-b-5)	(2-b-6)	(2-b-7)	(2-c)

Figure 6-5: Threats and Impact Area Assessment

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

The next step is establishing the likelihood factor for identified risks in the following Risk Likelihood Table.

Risk Likelihood	Descriptor	Description
1	Very Low	<ul style="list-style-type: none"> ▪ Highly unlikely, but it may occur in exceptional circumstances. It could happen but probably never will. ▪ It may occur once in 10 years.
2	Low	<ul style="list-style-type: none"> ▪ Not expected, but there's a slight possibility it may occur at some time. ▪ Likely to occur once in 5 years.
3	Medium	<ul style="list-style-type: none"> ▪ The event might occur at some time as there is a history of casual occurrence at the organization. ▪ It will occur once in 2 years.
4	High	<ul style="list-style-type: none"> ▪ There is a strong possibility the event will occur as there is a history of frequent occurrences at the organization. ▪ It will occur once a year.
5	Very High	<ul style="list-style-type: none"> ▪ Very likely. The event is expected to occur in most circumstances as there is a history of a regular occurrence at the organization. ▪ It will occur once in 3 months.

Figure 6-6: Risk Likelihood Table

Finally, we can deduce the impact of the risk on our organizational operation by multiplying the "rating factor" by the "likelihood of the risk." For example, we have identified tornadoes as a potential risk for our organization's Singapore and the Philippines operation. Based on the risk rating table, its impact on our operations is "3", but the likelihood of a tornado in Singapore is "0". Thus, the effect on our business operation is $3 \times 0 = 0$. This means that tornado is not a risk to our Singapore operation. However, the likelihood of a tornado in the Philippines may be "10". Thus, its impact on the Philippines operation will be $3 \times 10 = 30$, which is a significant risk to be addressed promptly.

In addition to the above numerical assessment technique, we should also consider the following areas to make the risk assessment more complete:

- The frequency of disasters is happening.
- Proliferation speed of the disaster from one location to the next.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Duration of the disaster.
- Existing and required redundancy levels of hardware, software, information and human resources throughout the organization accommodate critical systems and functions.
- Major consequences due to a disaster include personal injuries, loss of assets, loss of operational capability due to facility/equipment damages, legal liabilities, legal obligations, and financial penalties.
- Potential financial loss:
 - Increased operating costs;
 - Loss of business opportunities;
 - Loss of financial management capability;
 - Loss of assets;
 - Negative media coverage;
 - Loss of stockholder confidence;
 - Loss of goodwill;
 - Loss of income;
 - Loss of competitive edge; and
 - Legal actions.

Potential losses for each business function are based on the financial and service impact and the length of time the organization can operate without this business function. The impact of a disaster-related to a business function depends on the outage type and the time that elapses before normal operations can be resumed.



Figure 6-7: Risk Ratings and Risk Levels

6.5 Risk Treatment

Risk treatment is selecting and implementing appropriate options for dealing with risk. There are four possible treatments for risks.

Risk Avoidance

Make an informed decision not to become involved in or withdraw from a risk situation.

Risk Reduction (Mitigation)

Take appropriate actions to lessen the likelihood of negative consequences or both associated with risk.

Risk Transference

Shift the burden of loss for a risk to another party through legislation, contract, insurance or other means.

Risk Acceptance (Tolerance)

Make an informed decision to accept the probability and impact of a particular risk.

Risk Treatment	Description
Avoidance	Risk Avoidance is deciding not to become involved in or to withdraw from a risk situation.
Reduction	Risk Reduction is taking appropriate actions to lessen the probability, negative consequences or both associated with risk.
Transference	Risk Transference refers to shifting the burden of loss for a risk to another party through legislation, contract, insurance, or other means.
Acceptance	Risk Acceptance is making an informed decision to accept the likelihood and impact of a particular risk or pursue an opportunity. Risk Acceptance depends on risk criteria and the risk appetite of Top Management.

Figure 6-8: Description of Risk Treatment

6.6 Risk Avoidance

Risk avoidance is an informed decision not to become involved in or withdraw from a risk situation.

However, another related term, Risk Rejection, rather than understanding and embracing the risk, risk rejection denies that the risk exists. Risk rejection should seldom be an option

if the RA process has been executed carefully. However, the Executive Management ultimately decides what to do, and risk rejection occurs.

6.7 Risk Reduction

Risk mitigation is the most preferred course of action when an asset is critical and the risk is highly probable. Risk mitigation is selecting and implementing one or more controls to reduce risks to an acceptable level.

Controls typically operate to reduce either the exposure or the threat occurrence. It reduces the impact of the risk if it occurs or the probability that it will happen. Risk Reduction:

- Seeks proactively to avoid risk, not just react when/if it occurs
 - Attempts to reduce the impact of risks through planning and preparation
-

6.8 Risk Transference

Risk transference is transferring or shifting risk to someone or something else. The use of insurance is one option. Insuring against a risk transfers the potential monetary loss to an external agency. If the event occurs, the insuring agency will reimburse the organization for its financial loss. Insurance premiums are established based on the frequency and cost of each type of incident. Insurance is typically appropriate to deal with risks that cannot be eliminated, such as residual or risks with no possible control.

6.9 Risk Acceptance

An important issue in considering a response to risks is identifying the “risk acceptance” of the organization.

Risk acceptance is the amount of risks the organization is prepared to be exposed to before it judges an action as necessary. The fact that the resources available to control risks are likely to be limited means that value-for-money decisions have to be made – what is the appropriate resource cost to incur to achieve a certain level of control in respect of the risk? Apart from the most extreme circumstances, it is unusual that good value for money may be obtained from any particular risk being entirely obviated with total certainty.

Risk acceptance may be unequivocal about a particular risk or more generic because the total risks an organization is prepared to accept at any time will have a limit.

6.10 Risk Treatment Process

The risk treatment process encompasses various activities to identify, control and mitigate risks to an IT system and environment. **Figure 6-9: Threat Identification and Evaluation of Existing Controls** assist the Organisational DR Coordinator in identifying the existing Risk Treatment and controls. In summary, risk management is there to deliver the following two primary functions:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Prevent or reduce the likelihood of damaging incidents by reducing or mitigating risks. These preventive measures reduce or mitigate risks from the security controls that protect a system against natural, human and technological threats.
- Encompass actions to reduce or limit the consequences of threats if they successfully disrupt a system. These measures are developed in anticipation of a possible event and will be executed after that event occurs. Such procedures and processes form the basis for the DR Plan.

For a risk management process to work appropriately, strong Executive Management support and endorsement of disaster prevention and preparedness must be built. This will ensure that good and effective prevention or mitigation techniques and solutions can be adopted and applied to counter unwanted or unwelcome disaster circumstances.

This book explains some commonly available risk management techniques to mitigate identified risks to organizational operations.

S/N	Threat	Existing Risk Treatment				Existing Controls
		Avoidance	Reduction	Transference	Acceptance	
1						
2						

Figure 6-9: Threat Identification and Evaluation of Existing Controls

6.11 Procedural Prevention

Procedural prevention refers to operational activities performed daily, monthly or annually. Procedural prevention aims to define actions necessary to prevent various types of disasters and ensure that these activities are performed by competent and qualified personnel.

6.12 Physical Prevention

Physical prevention refers to special requirements for building construction and fire protection for various equipment components. The items for physical prevention include fire detection and extinguishing systems, air conditioning, heating and ventilation systems, electrical supply and UPS systems, and backup, archival and recovery systems.

6.13 Insurance

Although a well-prepared and tested DR Plan may not reduce the insurance coverage for IT systems, it can reduce risks and address many concerns of the insurance's underwriter. A good plan reduces the possibility of add-on premium costs or increases the acceptance of the insurance purchase.

Most insurance agencies specializing in business interruption coverage can provide the organization with an estimate of anticipated business interruption costs. Many organizations that have experienced a disaster indicate that their costs were significantly higher than expected in sustaining temporary operations during recovery.

The types of insurance coverage to be considered should include computer hardware replacement, extra expense coverage for system recovery and installations, business interruption coverage, valuable paper and records coverage, errors and omissions coverage, and media transportation coverage. With cost estimates collected from the insurer for each coverage, management can then make reasonable decisions on the type and amount of insurance to carry and the extent of losses the organization is willing to accept.

6.14 Outsourcing

Outsourcing some critical business support operations, such as email services or website hosting services, is a way of transferring risk factors to third parties. However, a comprehensive scope of work, expected service level, problem response and resolution framework, and the process must be established and proven workable before successful outsourcing. If this is not done, outsourcing can risk the organization's operations.

6.15 Records Keeping

Records can be divided into:

- Vital records, which record that cannot be replaced.
- Essential records refer to records that can be obtained or reproduced at considerable expenses and after some time delay.
- Useful records refer to records that may cause inconveniences when lost but can be replaced without cost.

The degree of impact in a disaster situation can vary depending on the different classifications of the records and the way and location of the storage. For example, records kept in standard metal cabinets are more liable to be lost in a fire than records stored in fire-resistant file cabinets. And, of course, it will be much safer for vital records to be held in offsite storage than in the office.

6.16 Other Control Measures

Some other measures that can be taken to deter, detect, and reduce the impact on the system are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls).
- Gasoline or diesel-powered generators provide long-term backup power.
- Air conditioning systems with adequate excess capacity to accommodate the failure of specific components, such as a compressor.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Fire suppression systems.
- Fire and smoke detectors.
- Water sensors in the computer room ceiling and floor.
- Plastic tarps may be unrolled over IT equipment to protect it from water damage.
- Heat-resistant and waterproof containers for backup media and vital non-electronic records.
- Emergency master system shutdown switch.
- Offsite storage of backup media, non-electronic records, and system documentation.
- Technical security controls such as cryptographic key management and least-privilege access controls.
- Frequent and scheduled backups.

6.17 Conclusion

Ideally, all identified risks would be eliminated. However, in practice, this rarely is a cost-effective option. So instead, an attempt is made to reduce risks to acceptable levels while remaining aware of residual risks. Residual risks could affect system performance, availability, integrity, and security.

Figure 6-10: Threat Impact and Likelihood Assessment (Part 1 and Part 2) will summarise the threats to the organisation.

The scope of the DR Plan may be reduced to address only these residual risks. In other words, the DR Plan can be more focused on conserving organization resources and ensuring an effective system recovery capability. Risks to the organization can vary over time, and new risks may replace old ones as a system evolves. Therefore, the risk management process must be ongoing and dynamic. Consequently, it is vital to analyze the costs related to minimizing the potential exposures as part of the DR planning process. Finally, the report is shown in **Figure 6-12: Risk Appetite and Recommended Risk Treatment**.

Threat	Impact Area					
	Financial	Processes (Business Operations)	Reputation and Image	People	Legal and Regulatory	Assets / ICT Systems / Information

Figure 6-10: Threat Impact and Likelihood Assessment (Part 1)

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Threat	Highest Risk Impact (Numeric)	Risk Likelihood	Risk Rating	Risk Level	Expected Period Of Disruption (Days)
	0		0		
	0		0		
	0		0		
	0		0		

Figure 6-11: Threat Impact and Likelihood Assessment (Part 2)

Risk Level	Risk Appetite	Risk Treatment (For Residual Risk)	Recommended Actions
Low	Tolerable	Acceptance	Manage using existing controls for monitoring.
Medium	Tolerable only with appropriate mitigation	Reduction Transference Avoidance	Specific strategies are needed. Management responsibility must be specified.
High	Non-Tolerable		Immediate action is required.

Figure 6-12: Risk Appetite and Recommended Risk Treatment

7 Business Impact Analysis



"We are in the business of meeting recovery objectives. Missing any objectives during a disaster is deemed a failure in our professionalism."

Dr Goh Moh-Heng

7.1 Objectives of BIA

Business Impact Analysis, or BIA, is a key step in DR planning. It enables the DR team to thoroughly analyze the system requirements, business functions, processes, and interdependencies. In other words, BIA allows the DR to establish priorities and priorities. A well-managed BIA process (Goh, 2008b) helps the DR Planning team streamline and focus their recovery strategy and development activities on achieving a more effective DR Plan. Such a plan will reduce disruption to the regular business operation, minimize legal liability, minimize loss, ensure orderly recovery and reduce reliance on key personnel. The three key objectives of the BIA process are to identify:

- Critical Business Functions (CBFs) and Applications.
- Disruptive Impacts.
- Recovery Priorities.

7.2 Identify CBFs and Applications

IT systems can be complex, with numerous components, interfaces, and processes. In addition, an IT system often has multiple missions resulting in different perspectives on the importance of system services or capabilities.

This first BIA step evaluates the IT system to determine its critical functions and identify the specific system resources required to perform them. See **Figure 7-6: Name, Code and Description of Business Function and Business Unit MBCO**.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

The following two activities are usually needed:

7.2.1 Step 1

The Organization DR Coordinator has to identify and coordinate with internal and external points of contact associated with the system and determine how they depend on or support the IT system. This coordination enables the system manager to analyze the full range of support provided by the system, including security, managerial, technical and operational requirements.

7.2.2 Step 2

The Organization DR Coordinator must also evaluate the systems linking these critical services to system resources. This analysis usually identifies infrastructure requirements such as electric power, telecommunications connections, and environmental controls. In addition, specific IT equipment, such as routers, application servers, and authentication servers, is usually considered critical. However, the analysis may determine that specific IT components, such as a printer or print server, are not needed to support critical services.

7.3 Identify Disruption Impacts

In this step, the Organization DR Coordinator need to analyze the critical resources identified in the previous step and determine the extent of the impact on IT operations if a given resource is disrupted or damaged.

Analyze and evaluate the impact of the outage in the following ways:

The effects of the outage may be tracked over time. This enables the Organization DR Coordinator to identify the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential business function.

See Figure 7-7: Identification of Impacts to Organization Due to the Unavailability of Business Functions.

The outage effects may be tracked across related resources and dependent systems. Identify any cascading effect that may occur as a disrupted system will affect other processes that rely on it.

7.4 Develop Recovery Priorities

The outage impact(s) and allowable outage times identified in the previous step enable the Organization DR Coordinator to develop and prioritize recovery strategies, and the sequence for recovering critical IT functions when the DR Plan is activated. For example, if the impact outage analysis determines that the system must be recovered within four hours, the Organization DR Coordinator must adopt measures to address that need. Similarly, if most system components can tolerate a 24-hour outage, but a critical component can only tolerate eight hours, the Organization DR Coordinator will prioritize the necessary resources to recover the critical components first. By prioritizing these recovery strategies, the Organization DR Coordinator may make more informed, tailored decisions regarding DR resource allocations and expenditures, saving time, effort, and costs.



7.5 Recovery Objectives

One of the most critical elements in the DR planning process is understanding the **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** for various IT functions. The recovery objectives provide the foundation for the entire DR Planning process and serve as a basis for BIA.

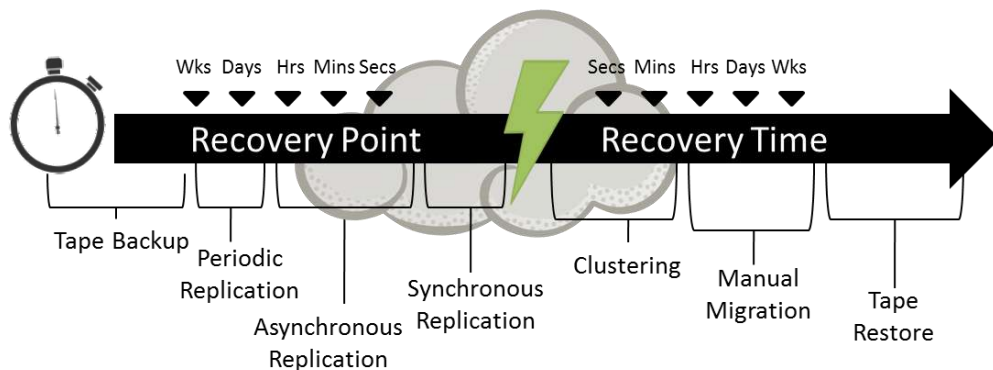


Figure 7-1: Recovery Point and Time Objectives

7.6 Recovery Point Objective

Recovery Point Objective (RPO) refers to the point at which data must be restored to resume the processing of critical business transactions.

For example, if your RPO is 6 hours, you want to be able to restore the systems to the state they were in 6 hours ago. One of the strategies to achieve this requirement will be to create backups or other data copies every 6 hours. Any data created or modified inside your RPO window after the last backup will be lost and must be recreated during a recovery. If your RPO is that no data is lost, online synchronous remote copy solutions may be the only choice.

7.7 Recovery Time Objective

Recovery Time Objective (RTO) refers to the minimum acceptable period within which critical business functions shall be restored and made available to continue critical business operations in the organization.

In other words, if the time taken to restore a resource is beyond its RTO value, it will adversely impact the organization. And the longer the RTO, the lower the cost for recovery.

For example, you might determine that customer service must function again after an interruption of one (1) day. Therefore, the RTO is one (1) day. On the other hand, you might decide that the RTO for your email system is four (4) hours. In some Internet businesses, an RTO might be measured in minutes.

It would help if you ascertained how quickly you require a particular IT application or system to be made available again. Otherwise, you cannot build a DR Plan that meets these critical recovery milestones. For example, a financial institution's most urgent IT needs are in its dealing room, as it can lose millions in just a few minutes should the IT facilities fail. Therefore, the recovery time for the dealing room IT facilities should be as short as possible.

Other functions (marketing perhaps), while important to the organization's overall strategy, are not critical during a DR. In fact, it may be possible to function adequately without your marketing business unit for hours or even days. However, a good understanding of your business operations' RTOs enables you to devise a plan to ensure a timely and effective business restoration.

It is essential to highlight that the results of the BIA enable the Organization DR Coordinator to determine the RPO and RTO for the recovery of mission-critical IT systems and applications. In addition, the RPO and RTO serve as reality checks for DR Planning, reminding you to focus on recovery essentials. For example, you may recover successfully with only 30 per cent of staff rather than your entire workforce; or cope with data that is 24 hours, rather than 24 seconds, old; or from a shared rather than dedicated recovery facility. Or perhaps you will need the instantaneous fail-over synonymous with high availability.

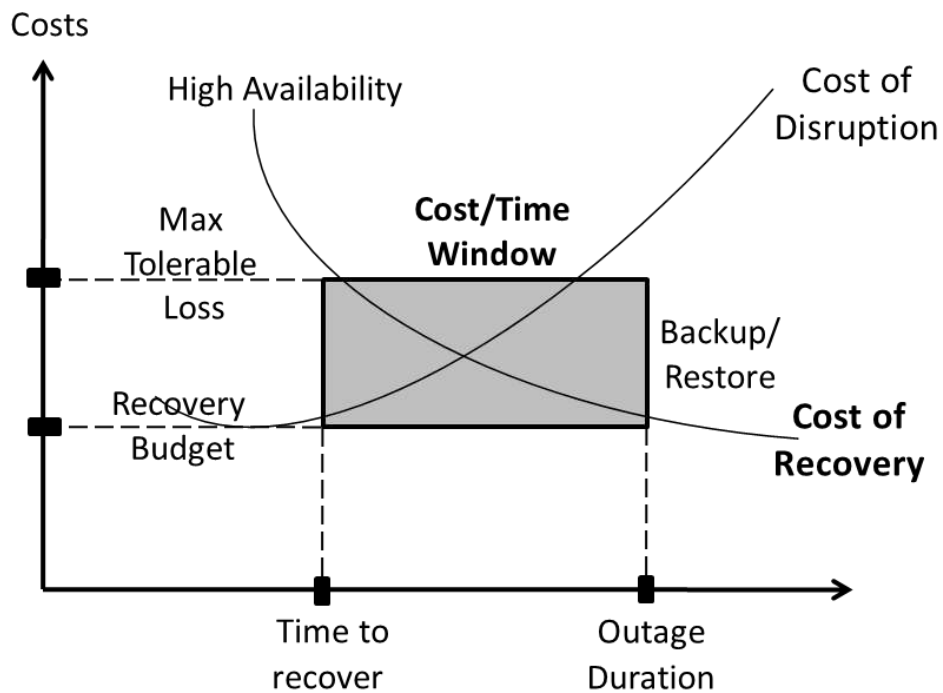


Figure 7-2: Recovery Point versus Cost

The BIA will determine the relevant RPO for each application or function, whatever your requirement. From this, you can ascertain how each part of the business would be recovered in case of an interruption, thereby developing a DR Plan tailored to the diverse recovery needs of your business.

7.8 Criticality RTO/RPO Tiers

RTOs are usually tiered by criticality. You'll need to look at your company's unique requirements for how many tiers are appropriate for your organization — more than five become unmanageable.

7.8.1 RTO Tiers

An example of the five RTO tiers:

Tier	RTO	Justification for RTO
1	No impact	Fault-tolerant with virtually no impact on the business users if the system goes down. Replication is part of the design of the system/application and usually requires a Tiered A RPO.
2	Less than 24 hours.	The system requires hot standby equipment and usually a Tier B RPO.
3	Less than 48 hours.	Test and development equipment takes on a production role in a disaster. This only applies when

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Tier	RTO	Justification for RTO
		a company has a second data centre with production running at one site and test and development running at the other.
4	Two to seven days.	Includes lower priority applications than tier 2 and 3. Supporting hardware can be either remaining capacity at a second data centre or hardware available via drop-ship arrangements with a third-party vendor.
5	More than seven days.	Requires acquisition of hardware and restoration of systems. Organizations determine RPOs based on the amount of data or transactions they can afford to lose.

Figure 7-3: Recovery Time Objectives Tiers

See Figure 7-8: Impact Over Time, Recovery Objectives and Priority for an example of RTO and MTPD.

7.8.2 RPO Tiers

These are the RPO tiers and their descriptions.

Tier	RPO
A	No data loss.
B	RPO of fewer than 24 hours.
C	RPO of last backup (24–36 hours in most cases).

Figure 7-4: Recovery Point Objectives Tiers

It would be best to define RTOs and RPOs whether you are recovering at your own alternate data centre or a cold or hot site operated by a third party. Third-party providers now have advanced recovery services that can meet high-availability requirements for RTOs and RPOs.

7.9 BIA Process

The BIA process will usually start with an organization-wide survey. However, you may say that this is impossible if your organization is a multinational organization with multiple domestic and international locations. Therefore, we suggest two ways to conduct surveys for more significant organisations.

7.10 BIA Initiation

Before the surveys or interviews, a proper briefing should be given to all Executive Management and business unit heads on the importance of BIA as an element of the entire DR Planning process and to be sure everyone is on the “same frequency”. This is a crucial process as it will enforce understanding on:

- Criticality of BIA towards the entire DR Planning process.
- BIA helps identify your business's needs as part of the enterprise-wide business continuity plan.

At the same time, this common understanding will help you to ascertain a realistic timeframe for you to carry out a complete BIA process, especially in getting the endorsement of Executive Management to commit resources. With Executive Management endorsement, you can gain staff participation in interviews or surveys to give you adequate information to assess each business unit's critical functions correctly.

7.11 Select Business Units

There are two approaches that an Organization DR Coordinator should adopt when identifying the business units which should be involved in the Business Impact Analysis (BIA) exercise.



If the Business Continuity Management team already conducts the BIA exercise, this exercise must be an extension of the BC process. For beginners, the vertical followed by the horizontal approach is a good and viable method.

See **Figure 7-9: IT Systems / Applications and Supporting Equipment** to identify units that require IT resources to recover their critical business functions

7.11.1 Vertical Approach

The start is to select a sample of business units that contribute to the organisation's daily operations, such as Sales & Marketing, Finance & Accounts, Investment, and Human Resources.

Next, interview the representative from these business units to determine which critical operations require support. You will thus be able to narrow down the key Executive Management and business units that must be included in the central nucleus of your BIA exercise.

7.11.2 Horizontal Approach

For this horizontal approach, participants are selected by making a horizontal cut across the organization's functional areas. This approach will survey a specific level of management that will produce a broad sample yet, small enough to remain manageable. However, this approach may create a negative impact of you running the risk of

interviewing people who might not know the critical requirements of the business, or they may not be able to quantify them and analyze disaster potential.

In summary, there are many possibilities for selecting your project population to be involved in the BIA survey. The key is to review and analyze your business processes, not simply automated ones. There is no perfect method for undertaking this portion of the project. All approaches have risks, scope problems, and time requirements. Your task is to minimize the risks while maximizing the results obtained from the enterprise and achieving a balance between the project and its cost.

7.12 Considerations for Interviews and Questionnaires

Some of the pointers for you to consider when you conduct interviews or survey sessions are listed as follows:

- Encourage quantifiable responses regarding lost revenue, periods, and liquidity damages payable.
- Vary the responses according to the expected time of potential failures, such as days, weeks and months, to see the likely patterns of damages varying with time.
- Plan for open-ended questions rather than closed ones, as it will enable you to learn informally enough about the critical processes of each business unit.
- Plan all questions and leverage the entire time scheduled for the interview.
- Use a standard set of questions across interviews with different business units to provide the necessary consistency between interviews and ensure that you have a base level of information to draw your conclusions later.

7.13 Interview and Questions

Interviews and questionnaires are the foundations for carrying out the BIA process. Therefore, the questions we formulate must be extensive and open to gain enough information and details to identify risks and impacts correctly.

Here are some excellent questions that you may want to consider using when you are planning the interviews/surveys:

- What are the core functions of the business unit in supporting the business operations?
- What are the necessary applications, information, tools or machines the business unit must have to function?
- Are any of these necessary items unavailable? Are there any alternatives?
- Can the business unit still function if any of the necessary items are?
- Is there any person in the business unit who is indispensable?
- What would you do without computing for x hours or days?
- Do you know if your data is backed-up daily, weekly, monthly, or annually?

- If so, how often? And are these data saved offsite?

7.14 Response Consolidation

After completing all the interviews and surveys, you can uncover a pattern of problems and vulnerabilities. And this is the ideal time to help the management understand what vulnerabilities need to be considered when developing the DR Plan.

When compiling the list of problems and vulnerabilities, be very specific in your definition of the problem or vulnerabilities and their solutions. It is best to list the details of each problem or vulnerability by topic and provide a corresponding detailed recommendation. Holding management's attention by recommending a solution(s) for each problem is always easier.

After completing the compilation of the interview notes, survey returns and projected losses, analyze the risk factors that have the most critical impact on the organization's business operations. In particular, think about the following factors,

- Unforeseen events can cause total or partial disasters affecting several people, facilities, and functions.
- Concentrate on any obvious and "expected" potential disasters. Most importantly, consider what needs to be done on a priority basis and what must be put in place for a smooth recovery.
- Pay particular attention to your organization's responses, especially those exposing weaknesses in your service environment.

A sample questionnaire for conducting Business Impact Analysis can be found in **Appendix I**.

7.15 Final Confirmation

After consolidating all these findings, review these findings with all the representatives you interviewed or surveyed to ascertain the correctness and accuracy of the results. Additionally, seek endorsement from their respective business unit heads before forwarding the BIA findings to justify DR expenditures, resources, and actions from the executive management.

Notes: BIA for critical business functions must be conducted (ISACA, 2012) before migrating to a cloud provider to assess the risk and define BCM requirements.

7.16 Conclusion

The Risk Analysis and Review (RAR) phase and the Business Impact Analysis (BIA) phase are two key phases within the DR Planning methodology to identify the risks from a list of potential risks and threats that will affect the organization's business operations. BIA ascertains the degree or level of impact on the business operations that the various identified risks will cause. Next, based on these identified risks and their respective impact, decide whether they can be deterred, countered or transferred via pure

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

preventive controls. Otherwise, a recovery strategy must be formulated, acquired, delivered and implemented. The process of formulation of the implementation of the recovery strategy will be discussed in the later chapters.

At the same time, we have also addressed in this chapter that risk Analysis and Review and BIA phases are not one-off exercises. It is a continuous process because IT systems, the environment, and business operations change over time. As a result, current risks may not be applicable anymore, and new risks will surface with organizational and economic changes. Hence, businesses need to ensure risk evaluation and business impact analysis are performed periodically, at least once a year.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/N	Business Function	Function Code	Description	Business Unit MBCO (Description)
Description	A business function is the business processes performed by the Business Unit. Please refer to Tab#8 and copy over the relevant Business Functions for your Business Unit.		A short description (less than 20 words) of the business function.	The minimum level of services acceptable to the Business Unit during a disruption. The BU MBCO must comply with legal and regulatory requirements and the company's MBCO and be measurable.
01	(example) Payroll Processing	HR-01	Process and disburse salary payout to employees	Payroll will be executed within T + 7 days.
02	(example) Recruitment	HR-02	Provide staff recruitment services	

Figure 7-6: Name, Code and Description of Business Function and Business Unit MBCO

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/N	Business Function	Function Code	Impact Area	Financial Impact		Legal And Regulatory Impact		Other Impact Areas
				Monetary Loss (Estimated)	Calculation of Monetary Loss (State Formula for Calculations)	Applicable Requirements	Area Of Compliance	Description
Description	Business function is the business processes performed by the Business Unit.	(BU)-01	1 Financial 2 Business Processes 3 Reputation and Image 4 People 5 Legal and Regulatory 6 Assets/ Systems/ Information	-	Calculation of monetary loss in SGD due to unavailability of business function for up to the planning time horizon.	Applicable or relevant clauses to be fulfilled.	Specify the particular area of compliance to take into consideration in BC planning.	This is to further explain how the unavailability of the department function will cause impact on other impacts, for example: 1. Damage to business reputation and image 2. Loss of business license 3. Loss of customer trust 4. Failure to deliver products and services on time 5. Adverse impact on outsource partners 6. Causing casualty on personnel
	01 (example) Payroll Processing	HR-01	Legal and Regulatory	-	-	Ministry of Manpower - Employment Act	Part III of Manpower Employment Act states that we need to pay salaries within 7 days after the end of the salary period.	-
	02 (example) Payroll Processing	HR-01	Reputation and Image	-	-	-	-	Damage to organisation's reputation and image

Figure 7-7: Identification of Impacts to Organization Due to the Unavailability of Business Functions

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/N	Business Function	Function Code	Highest Impact Area	Impact Over Time											RTO	RTO (Units)	MTPD	MTPD (Units)	Vulnerable Period	
				4	8	1	2	3	5	7	10	14	21	30						60
				Hours	Day(s)															
Description	Department Function is the business process carried out by the department.		The highest impact area amongst the relevant impact area(s) selected.	The impact of non-performance of the business function on the organisation. The Risk Impact ratings are as shown in Tab#9, Impact Descriptor															A particular period of the day / week / month / year in which the function is most critical or at its peak.	
01	(example) Payroll Processing	HR-01	Reputation and Image	1	1	1	1	2	2	3	3	3	4	4	4	3	Days	21	Days	20th of each month
02	(example) Recruitment	HR-02	Processes (Business Operations)	1	1	1	1	1	1	1	1	2	2	3	4	14	Days	60	Days	-
03																				

Figure 7-8: Impact over Time, Recovery Objectives and Priority

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/N	Business Function	Function Code	Supporting It Systems And Applications				Supporting Special Equipment or Resources	
			It Systems And Applications	Recovery Point Objective (RPO)	System Recovery Time Requirement			
Description	Department Function is the business process carried out by the Department.		Specific applications or systems are required to support each department's function—E.g. SAP, 1-OPS, Salesforce, Linux OS, NOVA etc.	If Others, please state	The point in time before a disaster to which system and data must be covered.	Is system recovery required to achieve RTO?	The period within which systems/applications must be recovered after a disruption has occurred to recover department functions.	Other office equipment and / or electronic devices required to support the department.
01	(example) Payroll Processing	HR-01	SAP HR Module	-	2 Hours	Yes	5 Days	-
02	(example) Recruitment	HR-02	Others	ARIS	-	-	-	-
03								

Figure 7-9: IT Systems / Applications and Supporting Equipment

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/N	Business Function	Function Code	Name Business Unit Or Vendor/Supplier/Outsource Partner - { X }	Type Of Dependency		Description Of Nature Of Dependency
				Internal/ External	Upstream to/ Downstream from the business function	
Description	Business function is the business processes performed by the Business Unit.		The internal BU or external vendor, supplier, or outsource partner with which each business function depends.			Indicate the nature of dependency and flow of information/transaction, i.e. hardcopy reports, faxes and emails between the BU and external parties for each business function.
01	(example) Payroll Processing	HR-01	All Business Units	Internal	Upstream	<u>All BUs</u> (Upstream) provide the updated list of employees to <u>HR</u> (Downstream) for payroll processing.
02	(example) Payroll Processing	HR-01	Finance	Internal	Downstream	<u>HR</u> (Upstream) provides the information on salary remuneration for processing to <u>Finance</u> (Downstream).
03	(example) IT Systems and Applications Support	IT-01	IT System Service Provider, Vendor XXX	External	Upstream	<u>Vendor XXX</u> (Upstream) provides system maintenance and recovery support to <u>IT</u> (Downstream).
04						

Figure 7-10: Inter-dependencies

8 DR Strategy: Data Backup



"The essence of the recovery strategy development is to continue key business and its information within the agreed recovery objectives."

Goh, Moh Heng

8.1 Overview

The Disaster Recovery Strategy phase is to identify the means to restore IT operations efficiently and effectively following a service disruption caused by any residual risks identified during the Risk Analysis and Review phase.

A good recovery strategy must address all the potential impacts identified during the BIA process. It can be integrated into the overall IT system architecture during its design and implementation phases.

The key considerations for developing a reasonable strategy cost, allowable outage time, security and ability to integrate with the enterprise-wide DR Plans. A recovery strategy can be achieved with one or a combination of multiple approaches that complement each other to provide the overall recovery capability to address the full spectrum of identified risks. In addition, the most appropriate recovery approach can be implemented on the IT system and meet its operational requirements.

The recovery approaches available include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service-level agreements with equipment vendors. In addition, IT technologies like Redundant Arrays of Independent Disks (RAID), automatic fail-over, Uninterrupted Power Supplies (UPS), and mirrored systems are viable recovery approaches that can be carefully considered. In the subsequent sections, we will detail the various recovery approaches you can use to develop your DR strategy.

8.2 Planning for DR Strategy

The primary aim of DR Planning is to respond to and recover from a disaster event efficiently. Thus, DR Planning focuses on minimizing the impact of an organisation's disasters. The typical strategies that are applied are as follows:

8.2.1 Avoid (or Prevent)

Implement baseline measures to ensure the security and reliability of activities and systems upon which the existence of an organization is highly dependent. Acquire or develop tools and techniques to eliminate bugs, configuration errors, and hardware failure.

8.2.2 Reduce (or Mitigate)

Implement measures to minimize the impact of unavoidable disasters or risks.

8.2.3 Respond/Recover or Anticipate

Identify the procedures to respond to and recover from disasters. This is achieved by predicting scenarios that are likely to result in a disaster, their likelihood of occurrence and their impact. Information for scenario formation is acquired from experience, the system's configuration deployed in the organization, problem logs, and audit reports.

8.3 Backup Strategies

The critical success factor for successfully implementing DR strategy is your ability to recover vital records, such as your necessary business data and application programs, not just your hardware, software and staff alone. The mechanism to ensure the continuity and availability of data and applications is to have a fault-tolerant set of backup and recovery processes to complement the complete DR strategy.

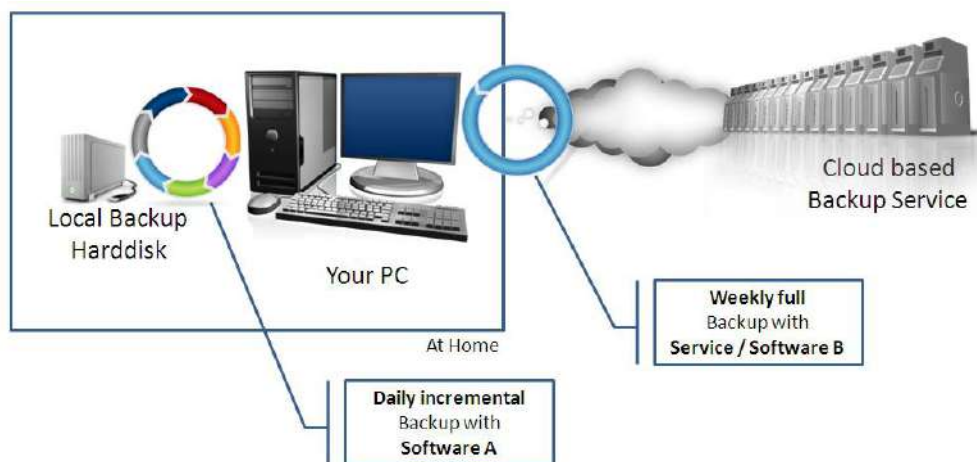


Figure 8-1: Backup Strategies

In general, all IT personnel today agree on all the following facts:

- Regardless of business data, system operational parameters, system guides, application programs, and so on must be backed up regularly.
- IT policies must be in place to specify the frequency of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced.
- Data backup policies shall designate the location of stored data, file-naming conventions, tape rotation frequency, and transporting data offsite.
- Data may be backed up on a magnetic disk, tape, or optical disk (such as compact disks [CD]). The method and media chosen for backup storage shall be based on system, data availability and integrity requirements. These methods include electronic vaulting, mirrored disks (direct access storage devices [DASD] or RAID), and floppy disks.

However, IT people need to understand the selection criteria for adopting the organisation's most suitable backup and recovery process to ensure the availability of critical digital assets during any disaster. This section will discuss a summary of the various backup and recovery options.

8.4 Data Type Classifications

Before selecting any recovery and backup process, there is a need to differentiate the data into classes, so that focus can be placed on understanding the level of volatility so that an effective and efficient DR Plan can be derived. The three different classes are application, infrastructure and system data.



8.4.1 Application Data

Application Data consists of general data that are required to run application programs. Such data includes application source codes, executable codes and business data in databases, text files, and working files, which are volatile.

The most critical set of application data is the business data, as it is the most valuable, most volatile and highly challenging to recreate compared to all other types of application data. The standard system change management process typically covers backing up application programs and system software changes. Ultimately, this adds complexity to the recovery of business data.

8.4.2 Infrastructure Data

This data class generally includes data required to interface operation systems to the application systems to provide a complete approach to service the users. These data have database management systems, security access, and control systems. Typically, this data class is subject to more frequent changes than system data; but is not as volatile as application data. At the same time, the standard System Change Management Process can control and manage infrastructure data.

8.4.3 System Data

System Data generally includes operating system software, parameters and configuration files required to “boot” the system or make the system operation-able. This data class is not subject to frequent changes or any such changes pre-planned and controlled by the standard System Change Management Process. Thus, it can be recreated if the worst-case disaster situation occurs.

8.5 Data Types

There are about five general types of data that you will need to consider and cater to when selecting the backup strategy to be adopted. The five data types are orphan, database, non-database-related, catch-up and loss data.

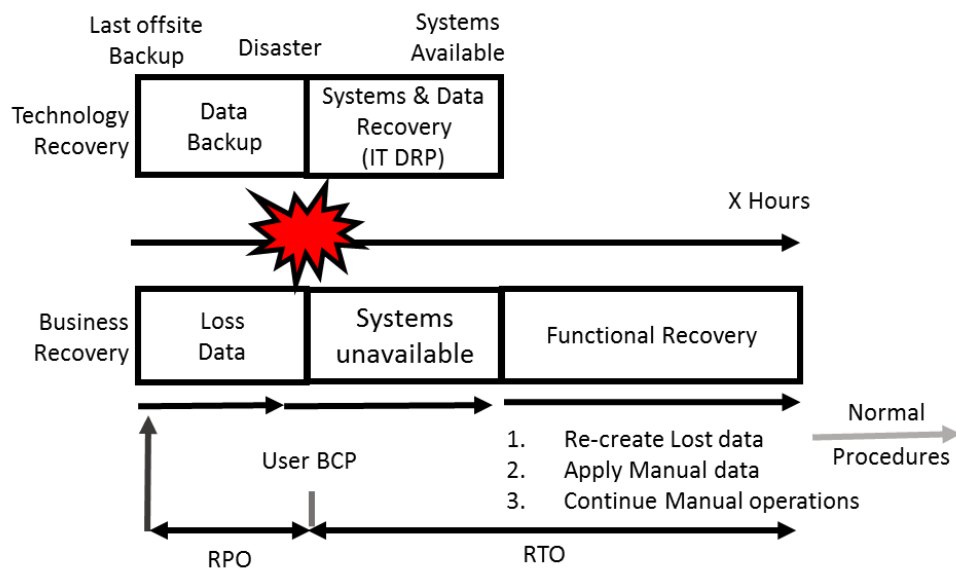


Figure 8-2: Technology versus Business Recovery

8.5.1 Orphan Data

Data updates are performed between the last data backup and when a disaster strikes. Thus, these data must be recreated to complete the system's recovery. Therefore, the volume of Orphan Data depends mainly on the frequency of backups and transfer to the off-site storage.

8.5.2 Database Data

Database data can reduce the amount of orphan data, as most relational DBMS provides log files that record all database updates committed. These log files are essential and facilitate the recovery of database transactions since the last full database backup. In addition, the log file size is small compared to the entire database; thus, such data can be easily backed up and transferred to off-site storage.

8.5.3 Non-Database Related Data

These are data made up of large sets of orphan data if the levels of data updates are very high. Thus, backup is needed more regularly and periodically to reduce data loss.

8.5.4 Catch-up Data

These are the business transactional data generated during a disaster, and they must be somehow entered into the systems after the system has recovered.

8.5.5 Lost Data

Lost Data is the data that is lost or cannot be recovered, and they exist in all DR plans. The amount of data loss depends on the backup and recovery strategy selected and the acceptability of the business needs.

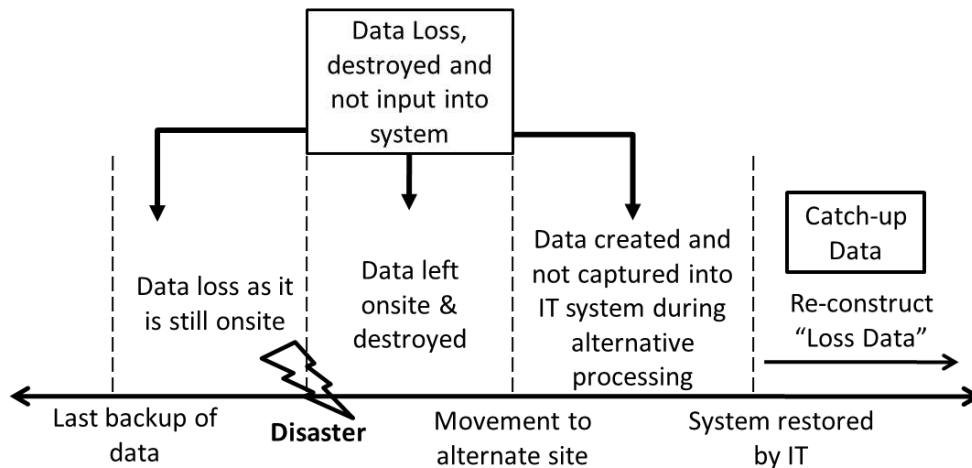


Figure 8-3: Overview of Data Loss Scenario

8.6 Data Safety Classifications

Data can only be considered to have been safely backed up when it has been successfully transferred to the off-site storage. There is always a possibility that backup media can be destroyed during an on-site disaster. There are two major classifications for data safety: Unsafe and Safe.

8.6.1 Unsafe

All forms of data that reside on the computer hard disk and are backed up onto backup media that are yet to be transferred to the off-site are considered unsafe.

8.6.2 Safe

Data that have been successfully transferred to the off-site storage and, better still, been restored onto the backup equipment that hosts the exact applications are considered safe.

8.7 Data Criticality Classification

The organization must determine what data is essential and how important each piece of information is - wasting time early in the recovery process recovering information that isn't as critical as other information is a less than effective use of resources. Instead, apply your efforts where they will make the most difference, especially early in recovery (whether it is a real disaster or a drill). Part of the planning process should include attention to which information has to be available and in what order to have the data ready for the users.

8.7.1 Critical Data

Critical Data is data to be retained and recovered for legal reasons. It is for the restoration of minimum work levels.

Within this definition of data, it is essential to note that the critical data necessary to restore minimum work levels is the data that should be concentrated upon first. You have to be able to access the data that needs to be retained for legal reasons, but that data does not necessarily have to be among the first recovered. The definition of minimum work levels is situation-specific, but among this information would likely be accounting information and access to purchasing, receiving, invoice processing, and payment processing functionality.

8.7.2 Vital Data

Vital Data is data that has to be retained and recovered to maintain normal business activities. This information and data represent a substantial investment by the organization in time and effort, and the recreation of the data may be difficult or impossible. This data may or may not be necessary for a disaster recovery situation. Necessity is determined situation by situation (the data in question, the criticality of the restoration, and the duration of the disaster all play a part).

8.7.3 Sensitive Data

Sensitive data is the data or documentation necessary for normal daily operations of the organization. However, there is a need to identify alternative sources of the same data or data that can be easily reconstructed from other readily available data sources.

8.7.4 Non-critical Data

Non-critical data is data that can easily be reconstructed at minimal cost or has its source in critical, vital, or sensitive data but has less stringent security requirements.

8.8 Types of Data Backup Strategy

Some commonly practised data backup strategies are full, incremental, and differential backups. In addition, there are the online DBMS data log, mirror, and hot backups.



8.8.1 Full Backup

A full backup captures all files on the disk or the folder selected for backup. A full backup is more reliable, eliminating the risk of omitting critical files. However, the full backup takes longer, utilizes more storage media, and demands more server resources and operator support.

8.8.2 Incremental Backup

Incremental backup is data backup executed on data changed since the last full data backup. These backup copies are only used together with the earlier full data backup.

Incremental backup reduces the copy time when the data updates are minor. It is not suitable where significant data portions are changed every day, as an incremental backup may take longer than a full copy.

8.8.3 Differential Backup

If a file is changed after the previous full backup, whenever a differential backup is performed, it will save the file each time until the next full backup is due. Recovering from a differential backup requires restoring the differential backup and the latest full backup. It takes less time than a full backup. The restoration may require fewer tapes than an incremental backup because only the full backup tape and the last differential tape would be needed. One disadvantage of differential backups is that restoration may take longer to complete than incremental backups because the number of data changes each time keeps increasing since the last full backup.

8.8.4 Online Data Backup

Online data backups are usually performed to avoid disruption or minimize system operations. This type of backup is very commonly used for DBMS, which allows the backup process to be executed while the databases are in use.

8.8.5 DBMS Data Log Backup

DBMS Data Log backup is a collection of all the updates made to a database, usually written to a file by the DBMS. This data log file is a critical file that will enable the DBMS to recover all the database transactions committed from the last database backup.

8.8.6 Mirror Backup

These backups directly copy all selected files, directories, mount points, and file systems from one set of disks to another. It is identical to a full backup except that the copied data cannot be compressed and is password protected.

8.8.7 Hot Backup

The system from the alternate site is in constant communication with the systems from the primary site.

In an emergency or disaster, connectivity to the systems automatically fails over to the backup site, and there is no downtime. In this scenario, an optimal solution for many organizations with multiple data centres or locations can be used as data centres.

9 DR Protection Strategy



"The essence of the recovery strategy development is to continue key business and its information within the agreed recovery objectives."

Goh, Moh Heng

9.1 Data Protection and Recovery Strategy

The data protection and recovery strategy mean data transfer between storage devices. As part of the DR process, it is critical as the sooner the backup data is accessed, the sooner the business operation can resume.

These are some of the categories for Data Protection and Data Recovery Strategy¹:

9.1.1 Data Backups

- Physical Offsite Vaulting
- Electronic Vaulting
- Remote Tape Vaulting

9.1.2 Replication

- Synchronous Replication
- Asynchronous Replication
- Data Replication
- Database Replication

¹ Source: www.bcmpedia.org – "Data Protection/Recovery Strategy – Category"

9.1.3 Mirroring

- Data Mirroring
- Disk Mirroring
- Remote Mirroring
- Remote Journaling
- Database Shadowing

9.1.4 Resilient Storage Implementation

- Redundant Arrays of Independent Disks (RAID)
- Redundant power supplies
- Redundant server connection
- Virtualization
- Cluster
- Network Attached Storage (NAS)
- Storage Area Network (SAN)

9.1.5 Cloud-based Disaster Recovery

- Do-It-Yourself
- Disaster Recovery as a Service (DRaaS)
- Cloud-to-Cloud DR

9.2 Data Backup (Manual and Electronic)

9.2.1 Physical Offsite Vaulting or Manual Transfer

Physical Offsite Vaulting is a traditional way. The backup media are transported from the primary site operation to offsite storage that may or may not be at the DR alternate site.

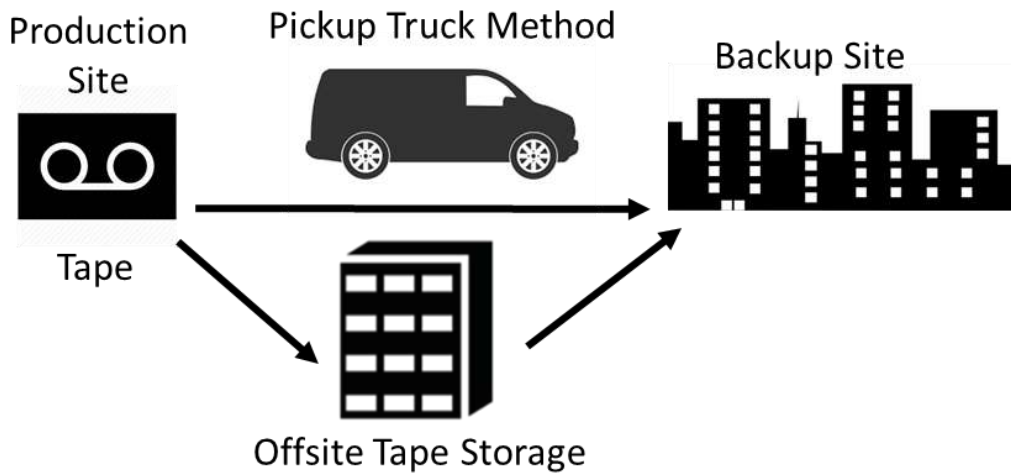


Figure 9-1: Physical Offsite Vaulting

9.2.2 Electronic Vaulting

This is a process whereby data are backed-up, and the output is electronically transmitted to a secured offsite storage location. This is usually done on batch processing.

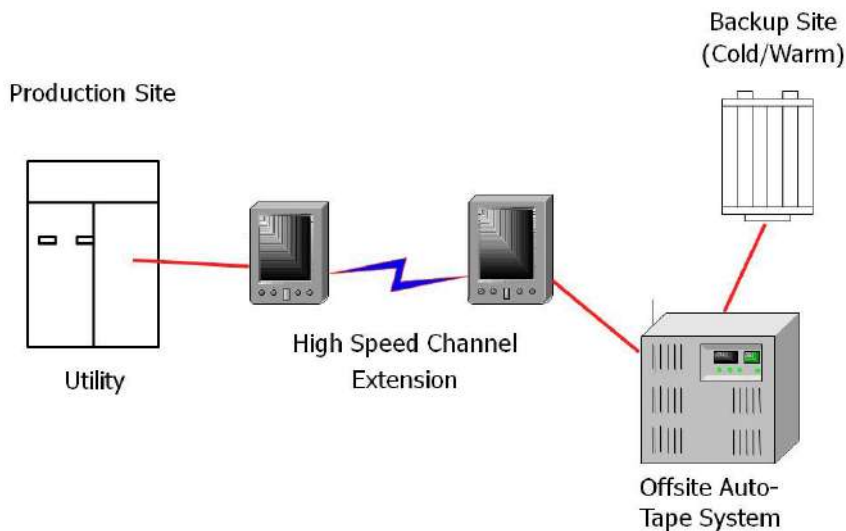


Figure 9-2: Online Tape Vaulting

9.2.3 Remote Tape Vaulting

Remote Tape Vaulting is the writing of data backup to a tape library or loader located at an offsite facility via and WAN or internet connection.

9.3 Replication

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

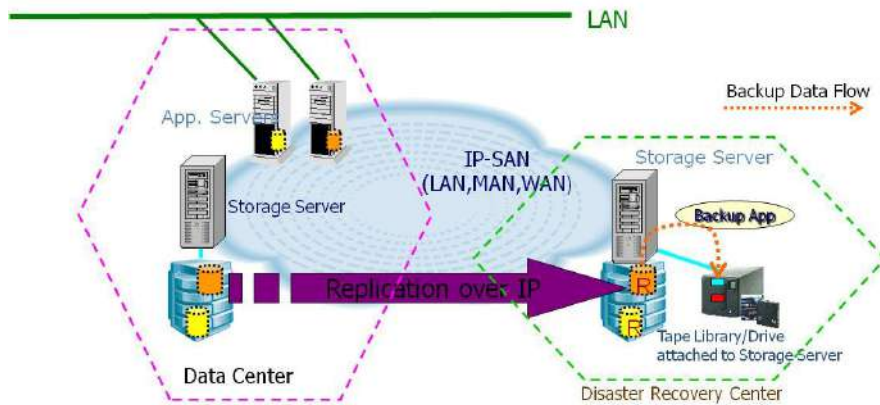


Figure 9-3: Replication

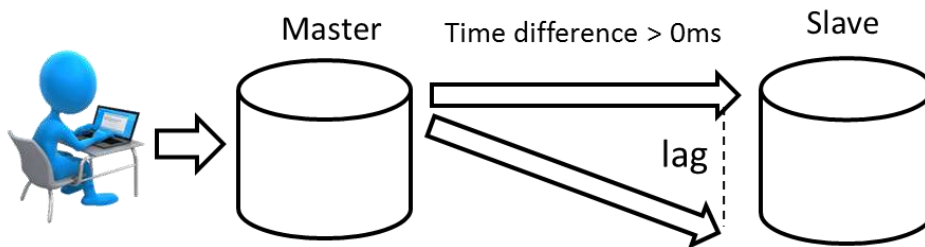


Figure 9-4: Asynchronous Replication

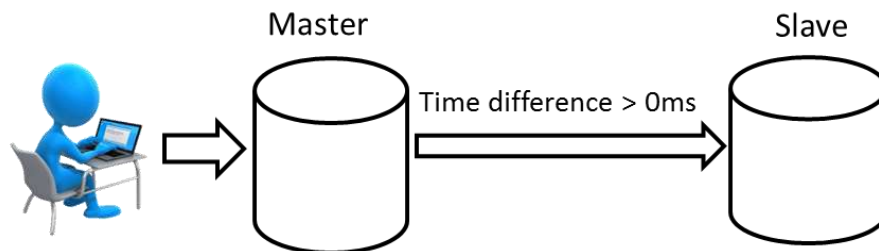


Figure 9-5: Synchronous Replication

9.3.1 Synchronous Replication

Synchronous Replication will only allow new data to be written to the storage sites when the previous data set is written to both the primary and the secondary (remote) storage sites.

The advantage of this approach is that the two sets of data are always synchronized. The disadvantage is that if the distance between the two storage disks is substantial, the replication process can take a long time, slowing down the application writing the data.

9.3.2 Asynchronous Replication

This replication process, as opposed to Synchronous Replication, is when the data has been written to the primary storage site, and new writes to that site can be accepted without waiting for the secondary (remote) storage site to finish its writes.

Asynchronous Replication does not have the latency impact that synchronous replication does but has the disadvantage of incurring data loss should the primary site fail before the data has been written to the secondary site.

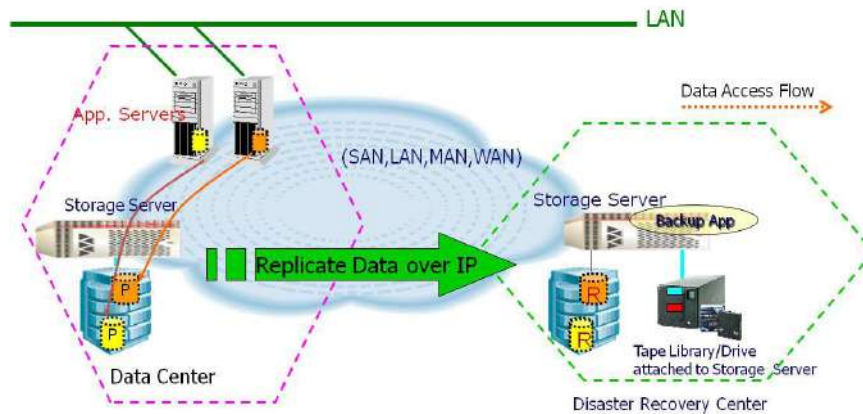


Figure 9-5: Asynchronous Replication over IP

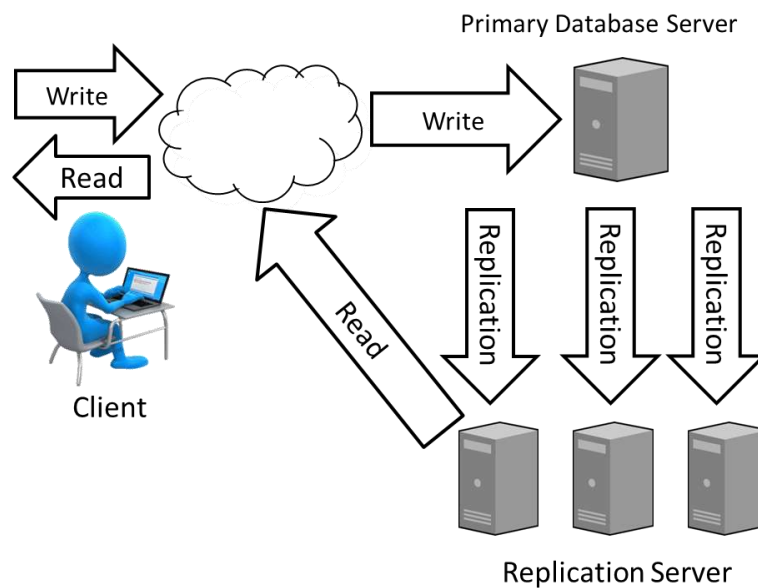


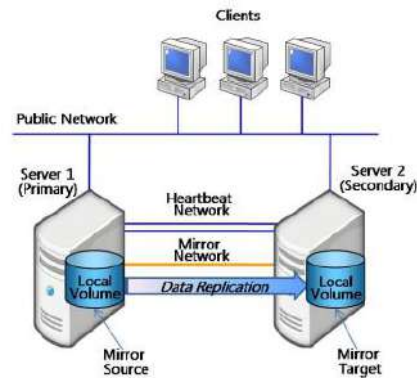
Figure 9-6: Database Replication

9.3.3 Data Replication

Data Replication is a scheme whereby data is copied from one site to another for disaster tolerance.

9.3.4 Database Replication

Database Replication is to make copies of the database for backup, performance, reliability, or preservation.



9.4 Mirroring

Mirroring is a strategy that maintains selected data such that both copies of the data (local and remote copies) are synchronized. Mirroring requires that updates to data be received at both the primary and secondary locations before the owning application is notified that the update is complete. Mirroring also requires dedicated hardware at both sites, which can automatically transfer the workload between sites. Using this strategy, virtually no data will be lost in a disaster, thus providing for continuous availability.

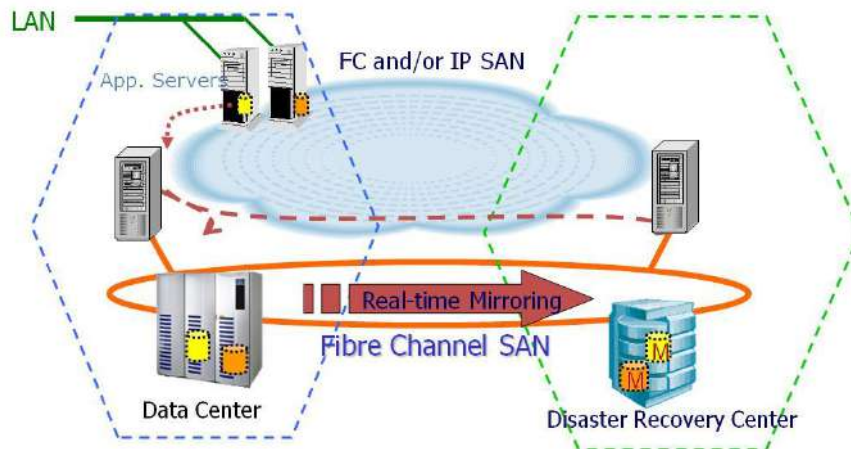


Figure 9-7: Real-time Mirroring

The two sites should be physically removed from each other and capable of handling regional disasters, such as floods or hurricanes.

9.4.1 Data Mirroring

Data Mirroring is copying data from one storage media to another in real-time so that there are always two copies of the same data.

9.4.2 Disk Mirroring

Disk mirroring is a two-disk system which is attached to a host controller. One of the disks will serve as the mirror image of the other. When data is written to one disk, it is reported to the other. Both disks will contain precisely the same information. Disk mirroring protects data against hardware failure. If one fails, the other can supply the user data without a problem.

9.4.3 Remote Mirroring

Remote Mirroring is the writing by the mirroring disk to the duplicate disk array located at an offsite facility via and WAN or internet connection.

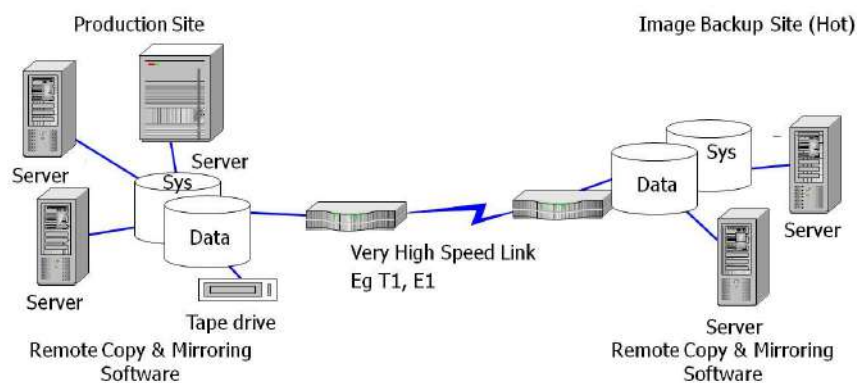


Figure 9-8: Remote Mirroring

9.4.4 Remote Journaling

Remote Journaling is the parallel processing of transactions to alternate site data storage via a communication linkage instead of a batch dump process (electronic vaulting).

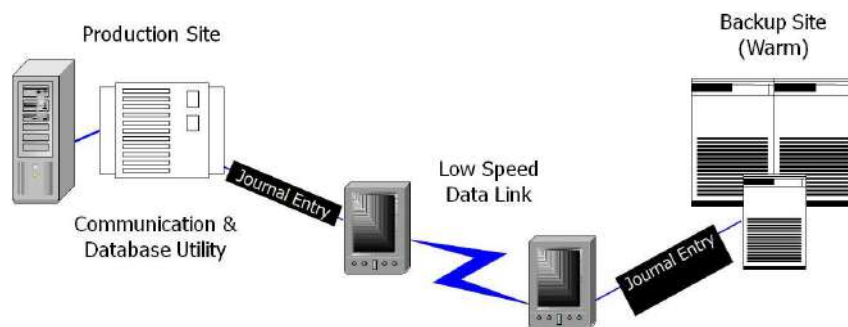


Figure 9-9: Remote Journaling

9.4.5 Database Shadowing

Shadowing is the live processing of remote journals, duplicated onto multiple database servers located at the alternate site data storage via communication linkages.

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

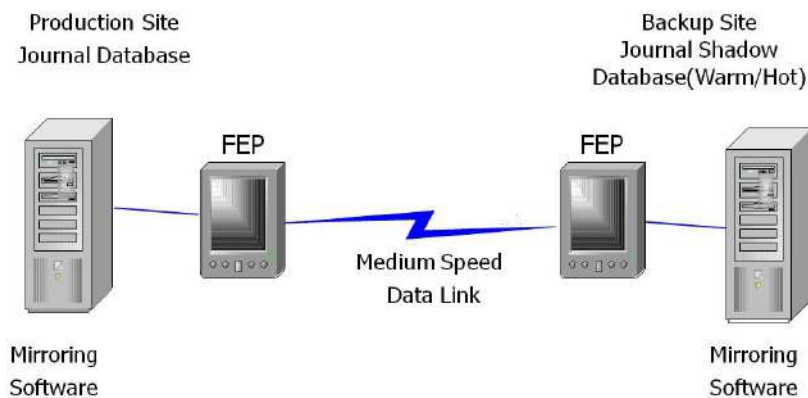


Figure 9-10: Database Shadowing

9.5 Resilient Storage Implementation

The failure due to storage often accounts for a high level of unscheduled downtime. In this section, implementing these storage technologies will reduce the likelihood of a lower-severity storage failure, such as equipment failure. However, this strategy will not enable an organization to recover should the entire storage system be unavailable.

9.5.1 Redundant Arrays of Independent Disks (RAID)

Redundant Arrays of Independent Disks or RAID is a group of disks configured to appear as a single disk drive to the host. These independent disks or RAID use many smaller disks instead of one large disk to store data. The reason is that this is a less expensive approach to using many low-cost drives as a group to improve performance, yet it also provides a degree of redundancy that makes the chance of data loss remote.

9.5.2 Virtualization

Virtualization combines multiple physical storage devices into a logical, virtual storage pool that can be centrally managed and is presented to the network applications, operating systems, and users as a single storage device.

Virtualization is associated with several computing technologies, including the following:

- Storage
 - The unification of multiple network storage devices into what appears to be a single storage unit.
- Server
 - The partitioning of a physical server into smaller virtual servers.
- Operating system-level
 - A type of server virtualization technology which works at the operating system (kernel) layer.
- Network

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Use network resources through a logical segmentation of a single physical network.
 - Application

9.5.3 Cluster

A cluster is a group of systems that work together as a single system to provide fast and uninterrupted services. It has sufficient hardware and software redundancy that a single failure will not significantly disrupt its services.

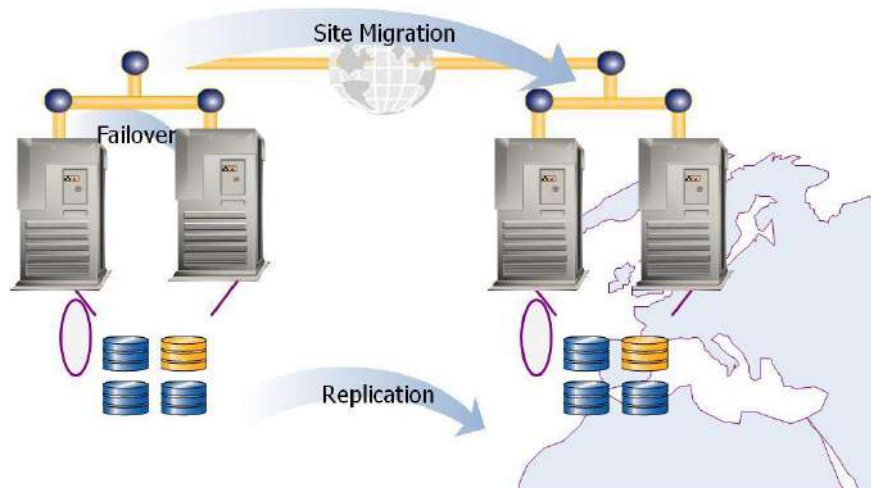


Figure 9-11: Server Clustering

9.5.4 Network Attached Storage

The Network Attached Storage (NAS) device is a server that runs an operating system specifically designed for handling files rather than block data.

9.5.5 Storage Area Network

Storage Area Network (SAN) is a high-speed specialized network that provides access to high-performance and highly available storage sub-systems.

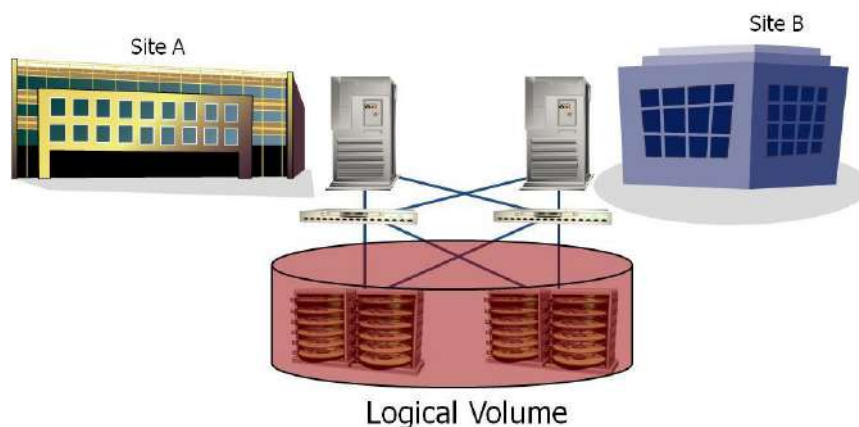


Figure 9-12: SAN Cluster



Replication is used when the RTOs are very short and RPOs very time-sensitive. Replication can be an asynchronous replication or synchronous replication. Synchronous Replication means the application will receive simultaneous confirmations for data written simultaneously to either disks or locations. Asynchronous Replication implies that the application will receive a confirmation from the primary write first and the secondary write later. The secondary write might be to an alternate site located a hundred kilometres away; thus, the confirmation of the second write will take longer. The reason for selecting the asynchronous replication option is to minimize the impact on the performance of the primary application (we do not need to wait for the secondary write before proceeding) as this machine is usually machine-critical.

In extending the options of synchronous replication and asynchronous replication, there are three possible levels of implementation:

- Host Level
- Replication be done at the servers level
- Array-based Level
- The use of storage array, e.g. Redundant Arrays of Independent Disks (RAID), and specialized software that will do array-to-array based replication.
- Fabric Level

Implementation is done in the fabric itself, for example, the SAN fabric or Virtualization, which captures or re-divert I/Os and goes to another fabric. Then, there is little reliance on a particular server or array.

9.6 Cloud-based Disaster Recovery

9.6.1 Do-It-Yourself

The organization is expected to manage and configure its solution using public cloud resources.

9.6.2 Disaster Recovery as a service or DRaaS

Per agreement to service levels, the organization will procure "pay-as-you-go" recovery services with specific RPO and RTO.

DRaaS is a cloud computing category that protects an application or data from a natural or human disaster or service disruption at one location by enabling a full recovery in the cloud. It is cloud computing's answer to DR.

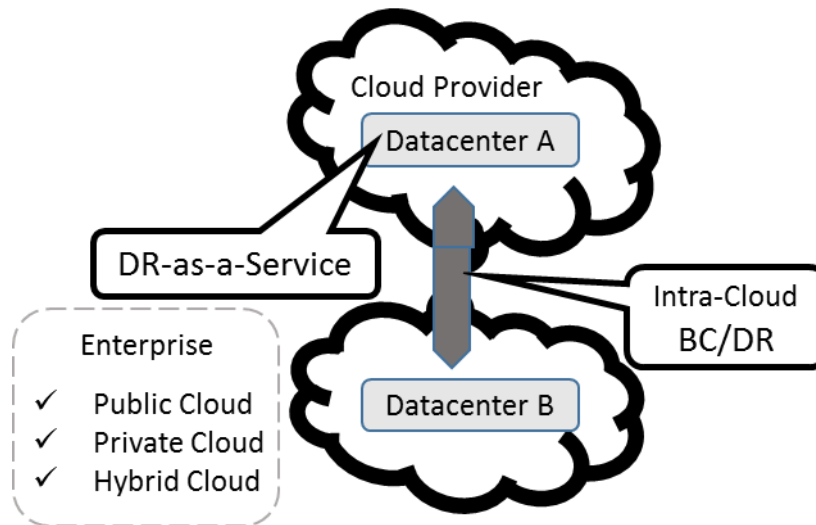


Figure 9-13: Cloud-based DRaaS (Gibilisco, 2014)

9.6.3 Cloud-to-Cloud DR

The ability to failover from one cloud environment to another.

9.7 Data Recovery Process

Performing a data recovery sequence always starts with restoring the backup datasets and applying all necessary updates. This is a logical and straightforward process. However, many organizations typically make assumptions and define operational parameters for the data recovery process based on in-house backup and recovery installations. Such assumptions are rather dangerous and may adversely affect the success of the recovery process.

It is important to remember that the backup or DR site's operational parameters will differ from the in-house environment. Therefore, extra considerations must be taken when one plans for its data recovery process.

Some of the critical considerations are:

- The compatibility of in-house backup hardware, software, and media with those at the recovery site.
- Data Consistency is the sequence for recovering each backup data set to maintain information consistency.
- Selection of a suitable data backup strategy (*Refer to 7.8*).

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

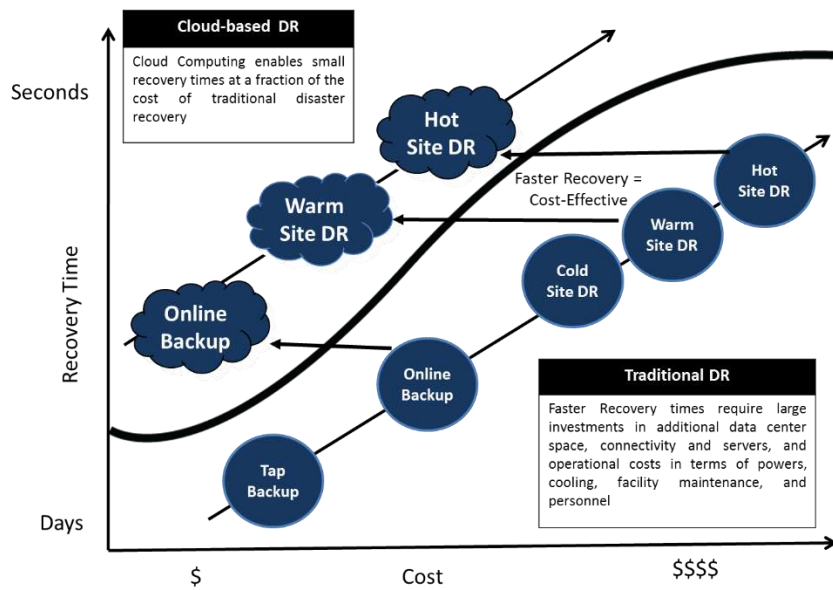


Figure 9-14: Cost versus Availability

In summary, the selection of an effective backup and recovery strategy is dependent on the following three major factors:

- Target recovery time means the shorter the recovery time and the more current the data have to be.
- The amount of data to be transferred, the larger the volume of data, and the most costly will be the telecommunication charges for electronic data transport between the in-house and off-site storage.
- The allowable data loss means where the data loss is less tolerable, the speed for data transfer and frequency of backup operations have to be increased. Thus, electronic data transfer methods will have to be applied compared to the slower manual data transfer.

9.8 Offsite Data Storage Options

It is a good business practice to store backed-up data offsite. However, regardless of what forms of data are stored on-site, there is always a possibility of being destroyed in a disaster.

Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. Where offsite storage is used, data is backed up at the organization's facility and then labelled, packed, and transported to the storage facility.

If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or an alternate facility. For example, commercial storage facilities often offer media transportation and response and recovery services.

When selecting an offsite storage facility and vendor, the following criteria should be considered:

Geographic Area

The distance from the organization and the probability of the storage site being affected by the same disaster event as the organization

Accessibility

The time necessary to retrieve the data from storage and the storage facility's operating hours.

Security

The security capabilities of the storage facility and employee confidentiality must meet the data's sensitivity and security requirements

Environment

The structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)

Reliability and Financial Status

The size of the customers, the nature of the organization's business, the P&L statements for the current and past years, and the organization's investment commitments on the off-site data storage business. And has the organization obtained quality certification and conducted annual third-party audits on the security and readiness of the off-site data storage facility

Legal Obligations

Any arrangement of third-party banker's guarantee to protect the customers from potential loss of data that are stored on the offsite storage should the organization liquidate or meet with any disaster

Cost

The cost of shipping, operational fees and disaster response/recovery services

9.9 Conclusion

When selecting options, the contracts and SLAs should include precise BCM requirements. This is especially critical when the organization selects a cloud service provider (ISACA, 2012).

10 DR Strategy: Alternate Sites



"The essence of the recovery strategy development is to continue key business and its information within the agreed recovery objectives."

Goh, Moh Heng

10.1 Alternate Sites Options

Alternate sites or facilities are required as part of the DR strategy to enable recovery and operation during a prolonged disaster. Although major disruptions with long-term effects may be rare, they should be accounted for in the DR Plan. In general, there are two main types of options for alternate sites available for consideration:

- Dedicated Site
- Reciprocal Site

Also, the two terminologies used:

- Primary site
 - A site whereby the primary IT infrastructure is located.
- Backup of Secondary site
 - An alternate or backup site to be used during a disruption or disaster.

10.2 Dedicated Site

A dedicated site owned or operated by the organization is a very costly option as it has to invest in building and maintaining an alternate site. This is fully equipped with all the necessary power, telecommunications, security mechanisms and hardware required to perform as a fully operational site, just like the main office, in case the main office is rendered un-operational should a disaster strike.

10.3 Reciprocal Site

The reciprocal site is to have a reciprocal agreement or memorandum of understanding with an internal or external entity. This agreement allows two organizations to back each other up. It is also sometimes referred to as a mutual-aid agreement.

Reciprocal sites can be drawn up between two similarly configured organizations. Each organization must have spare processing time, hardware capability, or amenity at a limited capacity to support the organisation's critical business functions and applications in distress. Large companies with many subsidiaries usually use these arrangements. However, enough spare processing time and equipment capability rarely exist to support a mutual recovery arrangement, even in these cases.

When negotiating a reciprocal site, there is a need to be extra cautious to review that each site must be capable of supporting the other. This is in addition to its workload and schedule, especially in a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized with a joint perspective.

10.4 Alternate Sites Recovery Strategy

In addition, there are four different types of Alternate Sites. They are cold sites, warm sites, hot sites and mobile sites. These alternate sites may be commercially leased or dedicated to an organization.

- Cold Site
- Warm Site
- Hot Site
- Mobile Site

The characteristics of each of these alternate sites will be discussed in the following sections, but keep in mind that regardless of the alternate site chosen, the facility must be able to support the system operations as defined in the DR Plan. To better understand the tasks to conduct a selection of the alternate sites, refer to **Appendix H: DR Site - Selection & Evaluation Checklist**.

10.5 Cold Site

Cold Site typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT systems. Space may have raised floors and other attributes suited for IT operations.

The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The cold site organisation is responsible for providing and installing necessary equipment and telecommunications capabilities.

The advantages of using a cold site are primarily lower costs and no potential resource contention with other organizations. However, the most significant disadvantage is the recovery time compared to other Alternate sites and no way to verify its workability until a real disaster strikes.

10.6 Warm Site

Warm Site is partially equipped with office spaces that contain some or all of the system hardware, software, telecommunications and power sources.

The warm site is maintained in an operational status, ready to receive the relocated system. Therefore, the site may need to be prepared for receiving the system and recovery personnel. A warm site may serve as a routine operational facility for another system or function in many cases. In the event of DR Plan activation, the normal activities are displaced temporarily to accommodate the disrupted system. The primary differences between a warm site and a hot site are:

- Applications on the warm site's equipment may not be installed or configured
- Datasets need to be restored from backup media
- Workstations and external telecommunication linkages may not be already available or configured in the warm sites

Compared to a hot site, the primary disadvantage of a warm site is the amount of time and effort required to resume operation. Thus, a warm site will not suit extremely critical transaction processing needs.

10.7 Hot Site

Hot Site is an office space appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel that work 24 hours a day, seven days a week.

A typical hot site will have:

- All applications that are needed to perform remote transaction processing
- All workstations are connected, installed and kept up-to-date with the latest configurations and software as in the existing working environment
- Typically, the hot site service provider will be notified to prepare for the data restoration process once a disaster is declared. When the organization's personnel arrive at the hot site, they will restore the last backup files and perform the data updates. Normal operation can be resumed at the soonest possible time. The recovery time can be further improved.



The primary advantage of the hot site is its 7 by 24 hours availability and exclusivity of usage. However, the disadvantage is its cost. Resources are needed to maintain consistency of hardware, software, configurations and applications at the hot site.

10.8 Mobile Site

Mobile Site is a self-contained, transportable shell custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements.

These are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and set up at the desired alternate location. To be a viable recovery solution, mobile sites should be designed in advance with the service provider. Service-level agreement (SLA) should be signed between the two parties. In other words, the time required to set up a mobile site can be extensive. Thus, prior arrangements and coordination are essential. This will ensure the delivery time of the mobile site during a disaster will not exceed the system's allowable outage time.

10.9 Differences in Alternate Site Recovery Strategy

There are cost and implementation time differences among the five options. Some of the key differences are as follows:

- A cold site is the least expensive to maintain, but substantial time is required to acquire and install the necessary equipment.
- A warm site is usually a partially equipped site and falls in the middle of the cost spectrum.
- The Hot Site is the most expensive choice, as it ensures virtually 100% availability.
- As for the mobile site, it may be delivered to the desired location within 24 hours.

Table 7-14 summarizes some considerations for selecting the most suitable Alternate sites for your organization. Alternate site selection cannot be made in isolation. It has to be considered in several vital areas, such as the required level of systems security, management, and operational and technical controls regarding firewalls and physical access controls. Also, bear in mind the compatibility between the prospective alternate site and the primary site.

Types	Cost Factor	Location	Recovery Time	Telecom Facilities	Hardware
Cold Site	Low	Fixed	Long	None	None
Warm Site	Medium	Fixed	Medium	Partial/ Full	Partial/ Full
Hot Site	High	Fixed	Short	Full	Full
Mobile Site	High	Not Fixed	Dependent	Dependent	Dependent

Table 10-1 Consideration Factors for Alternate Site Selection

10.10 Adoption Considerations

Alternate sites may be leased commercially or owned by the organization itself. If the site is to be operated by a commercial vendor, there is a need to observe the following adoption considerations of alternate sites:



- Is there sufficient testing time catered for?
- Is there an adequate workspace and workstations for both users?
- Are there sufficient security requirements catered for?
- Are all critical hardware requirements met?
- Are all telecommunications requirements met?
- Are there adequate support services available to support the recovery operation?
- Is the length of occupancy for the site clearly stated in the contract?
- Are there any established policies about prioritising and allocating facilities and resources should there be conflicts of more than one customer using the site?

10.11 Equipment Replacement Strategies

Strategies for swift procurement and delivery of hardware and software that support the operation of critical applications are critical to the DR process should the IT systems be damaged or destroyed or the primary site is declared unavailable or inaccessible in any disaster situation.

Three different types of strategies can be adopted to ensure the replacement of necessary hardware and software to support business operations. However, when adopting any replacement strategies, remember that transportation may be limited or temporarily halted in a catastrophic disaster.

10.11.1 Formalize SLA of Critical Applications

Establish a formal Service Level Agreement (SLA) with all the vendors who supply and maintain your hardware, software, and support services required to operate your critical business applications. This ensures commitment to response time to service, replace and deliver DR activities.

The key items to be indicated in the SLA should include the following:

- A detailed description of the hardware, software and support services required
- Vendor's response time after being notified or activated for the needed services
- Priority status of your organization for receiving a shipment of replacement equipment over equipment being purchased for normal operations and multiple clients

- Details of personnel that can be contacted
- A penalty for the vendors for not meeting the SLA
- Frequency of reviewing the content of the SLA

10.11.2 Warehousing of Critical Equipment

Warehousing of required critical equipment may be adopted by purchasing and storing them in advance at remote and secure offsite locations, such as:

- An alternate site where recovery operations will occur (warm or mobile site).
- A remote location from the primary site, and then shipped to the alternate site during a disaster.

The main drawback of this strategy is that it requires the organization to commit financial resources to purchase the equipment in advance. In addition, the kit may become obsolete or unsuitable for use over time because system technologies and requirements change.

10.11.3 Leverage on Compatible Equipment

This strategy will leverage any compatible equipment currently available at the contracted hot site or in another business entity of the organization to lower the cost of backup facilities. However, this strategy depends heavily on agreements established between the DR services vendors or reciprocal agreements with another business entity to ensure they are committed to providing these resources or equipment when needed.

When evaluating the different strategies for adoption, you must weigh the cost of the effectiveness and efficiency. For example, making equipment purchases after a declared disaster may seem less costly. Still, waiting for the shipment to arrive before the equipment can be set up will significantly add to recovery time. Although storing unused equipment is very costly, it allows recovery operations to begin quickly. Thus, you have to depend on the impacts discovered through the BIA, the possibility of a widespread disaster requiring mass equipment replacement and potential transportation delays to decide on a strategy for adoption.

10.11.4 Crate and Ship of Critical Equipment

Crate and Ship is a critical equipment strategy to have a contractual service level agreement with an equipment supplier to ship replacement hardware within a specified period. Another similar term used is called Quick Ship or Drop Ship.

10.12 Conclusion

Strategy identification, selection, and adoption with the correct personnel and sufficient financial resources are essential to successfully implementing the DR Plan. Remember that the cost of adopting each type of alternate site, equipment replacements, and storage options must be weighed against budget and resource limitations to adopt the most effective and efficient recovery strategy.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

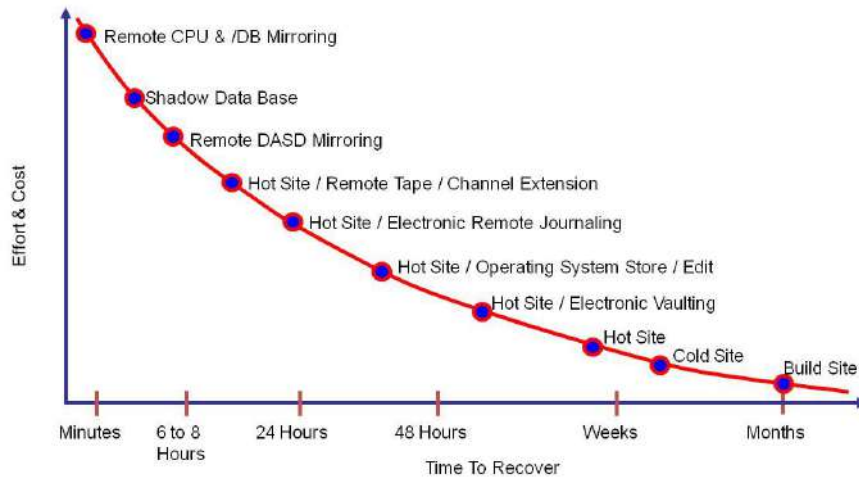


Figure 10-2: DR Trends

With the identified strategy, you will have to streamline all the costs and budget for software, hardware, travel and shipping, testing, plan training programs, awareness programs, labour hours, and other contracted services. In addition, any other applicable resources (e.g., desks, telephones, fax machines, pens, and paper) for you to implement the recovery strategy accordingly.

In summary, readers may find the following Appendices useful for their supplementary readings.

Appendix	Technical DR Considerations
A	End-User Computing
B	Servers
C	Local Area Networks
D	Wide Area Networks

Figure 10-3: Technical DR Considerations

11 Tender Evaluation and Award of DR Services

11.1 Overview

In the previous chapters, we discussed identifying the DR needs and establishing a DR strategy to address the DR needs. This chapter will focus on communicating the selected DR strategy and requirements to third parties (**Vendors**) outside the organization. This will enable them to propose the mechanism to generate the selected DR strategy within scope, cost and timeline.

The most challenging part in developing the Request for Proposal (RFP) is the information consolidation and presentation to ensure that Vendors understand your requirements and deliver solutions to meet them.

Request for Proposal is the publication of a document that invites and informs prospective vendors and service providers on the type of services or products a company is attempting to purchase or procure.

An RFP is a solicitation for potential contractors to submit their bids in a competitive process.

Some of the critical points that need to be explicitly communicated, clearly and precisely to the Vendors so that they can design and deliver a solution for you are as follows:

- What do you have today?
- Where is your organization's presence?
- What do you want to achieve?
- When have you tried to implement the identified DR strategy?
- How can the vendor assist you in achieving your above objectives?

In the following sections, we will share the process, from developing a DR Planning RFP to evaluating submissions from vendors and awarding the contract.

11.2 A Complete RFP Lifecycle

A well-written RFP must be a correctly structured document that is clear and precise. It should be readily understood and require minimum clarification. This is a crucial concept because a good RFP document will enable you to select and engage the most competent and effective Vendor, who will be able to deliver the DR strategy that you have identified within scope, schedule and budget. In summary, you can save your organization much time and money by ensuring that your organization's requirements are written down precisely.

A good RFP document can be developed by following a structural RFP lifecycle that encompasses three major stages: Pre-RFP, Development, and Post-RFP.

11.2.1 Pre-RFP Stage

The time and effort required for this phase depend mainly on your organisation's experience in managing the DR Plan. It will be shorter and require less effort if the Organization DR Coordinator has completed a DR Plan using the seven DR Planning cycles.

The major steps that need to be taken in the Pre-RFP stage are as follows:

The first step is to understand the market norm, what other people are doing, who are the good and bad DR Vendors, and what are the better DR facilities. This can be achieved through:

- Attending conferences, seminars and courses.
- Talking to key DR vendors and DR consultancy services providers.
- Talk to your peers and business contacts who have DR Plans in place.
- Asking for elementary or "budgetary" quotations for DR services vendors.
- Browsing professional DR or Business Continuity websites

This step is very critical to a newcomer to the field of DR, as it will help in:

- Understanding the current market trends, needs, practices and expectations of DR services.
- Distinguishing who the leading and established DR services vendors are.
- Making clear the critical DR components to Vendors to ensure a minimum level of DR services can be delivered.
- Understanding minimum expectations to be established in the RFP document.

If possible, try to pre-qualify vendors in this stage, as it will save time and effort to select the most suitable DR services provider for your organization. However, be very careful here, as you must establish a compelling justification for doing so in the Pre-RFP stage. This is because you must demonstrate to your management that the short-listed vendors are the most suitable, and there is no biased feeling of favouritism during the evaluation process.

11.2.2 RFP Development Stage

This is the main body of this RFP lifecycle. It involves the calling of RFP, collecting proposals, evaluating them, conducting proposal negotiations, and finally, awarding RFP to the successful Vendor.

11.2.3 Distribution of RFP Document

It is vital to ensure your RFP document reaches all your pre-qualified vendors and they know their proposals submission date to you to receive all your expected proposals in time. Therefore, you may want to pre-empt these Vendors with a single point of contact, place, date and time to collect and submit your RFP document and their proposals, respectively, through email, telephone or fax.

Suppose you feel more comfortable going through your RFP document with the Vendors to reduce the risk of uncertainty and misunderstanding of requirements and to address any potential yet common queries with Vendors. In that case, you may want to conduct a briefing for all Vendors. During the briefing, you may want to stress some of the following pertinent RFP requirements so that all vendors know exactly what you want out of their proposal:

- Specific technical requirements
- Legal terms and conditions
- Closing date and time
- Contact person
- Submission format

11.2.4 Establish the Deadline for RFP Proposal Submission

Setting a reasonable and comfortable deadline for RFP submission will ensure Vendors have enough time to propose a workable and effective solution for you. You will be able to collect the Vendors' proposals in time and reject all those who do not meet the deadline on the fairground.

11.2.5 Review and Shortlist RFP Proposals

This is a tedious step, as you must establish an evaluation strategy, selection criteria and pricing comparison framework to ensure a fair "apple-to-apple" comparison of all submitted proposals. Sometimes, you may want to establish a proposal evaluation committee to help you complete the proposal evaluations. Therefore, it is essential to communicate the selection criteria and evaluation strategy to all committee members to achieve a fair review.

You must carefully read all the proposals submitted before short-listing those that have met all your fundamental or mandatory requirements, cost, and delivery schedule.

11.2.6 Schedule Vendor Presentation

Provide a presentation schedule, guidelines, and the allocated time frame for each short-listed vendor. They have just enough time to present the core of their proposed solution and not too much to advertise their organization and credentials. Always have enough time to clarify uncertainties and confirm pertinent points that you may have after reading their proposal.

Also, ensure you have given yourself and your evaluation committee enough time between presentations to discuss the plus and minus of each Vendor internally before going on to the next.

11.2.7 Review and Award the RFP

After concluding the vendor's proposal, the proposal evaluation committee should jointly put up an approval paper to seek management's consent to award the RFP.

11.2.8 Notify Vendor of RFP Results

Upon obtaining your management's approval for the award of DR services, formally inform the successful vendor through a letter, fax or email. Always make it clear to the Vendor that the award is subject to mutual acceptance and final negotiations on the proposed items.

11.2.9 Finalize the Award

Negotiate and finalize the contract's scope, schedule, milestones, deliverables, and pricing with the successful vendor. In most cases, you must involve your legal personnel in the negotiation if there are legal issues.

11.2.10 Post-RFP Stage

You will need to establish the complete schedule with major milestones, expected delivery outcomes, major resource requirements, and the implementation strategy for your identified DR Strategy.

11.3 Major Components of the RFP Document

Request only relevant and not extensive information to your requirements to obtain the most appropriate and effective solution from the RFP process. Thus, consider what you want for your DR services with the corresponding evaluation criteria for the expected resources when you list the clauses on requirements in the RFP document. This section will share some of the critical items to be included in the RFP document. A sample table of content for an RFP can be found in **Appendix J**.

11.3.1 Administration Instruction

Write down the critical administrative details and organizational rules that all vendors interested in participating in the RFP submission need to be observed. These instruction details are listed in the following subsections:

11.3.2 Time Requirements

State clearly and specify precisely the RFP closing date and time so that there is no excuse for any Vendor to get the submission date and time wrong. If you permit an extension of the closing date and time, mention it in your RFP, state the circumstances upon which an extension will be granted, and the deadline for submitting requests for extension.

11.3.3 Location for RFP Submission

Indicate the address and tender box number for submitting the RFP document. This helps to ensure that the vendor can deposit the RFP document into the correct place by the stipulated time.

11.3.4 Respond Format

It should be stated clearly with a sample of the exact proposal format you want your vendor to compile and present their RFP proposal. Also, indicate the number of printed copies required and several soft copies in "doc" or "pdf" format stored in DVD-ROM or memory sticks.

With the standard format in place, it will be easier for you to evaluate and compare the proposals from different vendors. It is also a sound basis for establishing a common practice for the evaluation committee.

11.3.5 Pricing Structure

State precisely how you want the vendor to present their fixed or total fee price structure based on time and material.

11.3.6 Contact Point

A single point of contact to ensure consistent and unique responses to all Vendors' queries has to be established before the issue of the RFP document to all the vendors. Provide the name, email address and telephone number of this single point of contact in the RFP document.

11.4 Other Administrative Details

You must indicate other administrative details, such as those you think will impact the Vendors' resources and planning for their estimated project schedule. These are some of the items to be considered.

11.4.1 Presentation of Proposal

- Project the interviews required for the core DR team personnel of the Vendor
- Conduct site visits to the proposed DR site
- Have a good understanding of the benchmarking process

11.4.2 Rights of the Organization

State the specific rights that your organization expects from all vendors that want to participate in submitting proposals. If you think there is no ground for negotiation on your organization's rights, you may also want to stress that these are mandatory requirements that all Vendors must comply with fully; otherwise, their proposal will be disqualified.

11.4.3 RFP Decision

The RFP document commonly states that the organization reserves the right to accept or reject any RFP proposals it receives. The organization does not need to provide any reasons or explanations on the principle of the award to any of the vendors.

11.4.4 RFP Preparation Costs

Indicate clearly to all Vendors that all direct and indirect costs incurred by them before signing the official contract document between the vendor and organization must be borne solely by the vendor and that your organization will not pay any of these costs.

11.4.5 Ownership of RFP and Submitted Proposals

The vendor should be informed that all information listed on the RFP document will be copyrighted to your organization. However, in cases where you feel the information is critical, you may state in the RFP that no photocopying of the RFP document is allowed. Also, you may request that copies of the RFP document be returned to your organization with the proposal submission.

If you want to retain the rights for the RFP proposal submissions you receive, you must state and declare your intentions in the RFP document.

11.4.6 Presentation and Demonstrations

It should be stated clearly that your organization reserves the right to request for presentation by vendors on their proposal, visit the proposed site, view demonstrations of their offered products, etc. However, you must provide sufficient notice for the vendor to prepare and present their proposed solution, products, and services to you.

11.4.7 Verification of Qualification

State clearly that your organization reserves the right to interview any of the proposed individuals on their proposal or verify the credits of the vendor with any of the references provided.

11.4.8 Terms and Conditions

Indicate the standard contractual requirements, usually recommended by your internal legal advisors, for the Vendors to comply with. Some of the commonly used contractual requirements emphasize service quality and continuity and are dictated in many RFPs provided in the followings:

- Safeguarding of Information to ensure all sensitive information to your organization is protected.
- Liquidity Damages are required to protect your organization if the vendor cannot deliver the DR services or breaches the terms and conditions of the agreement.
- Transition commitments you need the vendor to honour and fulfil if there is a transition between the current vendors to another when the contract ends.
- The vendor has to provide a period of warranty so that any refinement to the DR Plan or setup can be done without additional costs to the organization.
- Banker's guarantee from the vendor to reinforce the vendor's commitment.
- Payment methods and schedules adopted by your organization are to be agreed to by the vendor.

11.5 Introduction to RFP

Provision of good background information on the history of DR activities in your organization, the rationale for your request for an RFP, and your organization's IT roadmap or vision that have a bearing on the scope of RFP will help the Vendor design a more suitable solution for your organization. We will review some of the information with you in the following sections.

11.5.1 Corporate Overview

It is always helpful to inform the vendor about the criticality and dependency of the organization's business operations on IT services. Some of the following points are worth highlighting to the Vendors:

- Your organization's core business, mission statement and core value statements
- Relationship between it and business units
- A high-level organization chart to indicate the reporting structure
- The extent it is used in the organization to support business operations

11.5.2 Scope of Services

Define the extent and coverage of this RFP so that Vendors are clear on what to deliver to your organization. The information to be written down should include:

- Tangible objectives for calling this RFP
- Lines of business and their international overseas presence, and which of them are included in this RFP?
- Key criteria, such as your expectations in determining the success in implementing the proposed solution

11.5.3 Requirements

At this point, you should provide a more detailed description of the scope and objectives that you have briefly mentioned in the introduction section of the RFP. The level of detail to be presented must be sufficient for the vendors to formulate and package their proposed project approach, resources, and timeline to meet your expectations. For example, the information should indicate whether there's already a DR Plan in place when it was done when it was last updated, the schedule of the previously completed test, etc.

11.5.4 Business Specification

Indicate any dependencies between the supporting business applications and daily business functions. State the tolerable downtime, user base regarding location and size, and business functions in the sequence of the level of criticality. You may want to include information on some of the following areas under the business specification:

- What are your project resources and their availability to participate with the vendor to deliver the DR strategy?
- What will be the project management methodology you will expect from the vendor if you have one? For example, a methodology equivalent to the ISO9000 IT project management standard.
- What project management status reporting and escalation procedures will you expect from the vendors or give to them?

Be specific about your requests and expectations regarding the vendors' description of their project approach, deliverables and timeline. Indicate the degree of detail you require on the significant tasks and relative effort and involvement by resources and consultants from both the vendor and the organization.

11.5.5 Technical Specification

Provide technical details such as the scope, functions, size and configuration of each IT application in your existing environment and how these technical components need or are expected to be recovered. Some of these technical items include:

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

- Application software: the name and version of the application software, the system software that it operates on, and the provider or manufacturer of the application software
- System software: the name and version of the application and the provider or manufacturer of the system software
- Hardware: detailed configurations (CPU, RAM, and hard disk size) of the servers and desktop PCs
- Data centre network: a detailed list of the network setup including physical number, brand, model, made and manufacturer of routers, switches, hubs, concentrators, repeaters, and modems.
- Dedicated / Leased lines: a detailed list of the physical number, types, speed and providers of all leased lines, ADSL lines, MPLS connections, and dial-up connections.
- Geographical coverage: the locations and how they are all inter-connected for information exchange and access
- Overall IT infrastructure configuration diagram

11.5.6 Qualifications

Request the vendor to provide a short write-up on its organization's setup, including:

- Vendor's name
- Vendor's address
- Vendor's core businesses
- Vendor's past turnover and investment in the DR services as compared to the other business, if any
- Vendor's presence in the rest of the world
- Vendor's prior experience in delivering a similar scope of DR services
- Certification and qualification of the organization individuals who will be providing the proposed solutions

11.6 References

Request for a list of customer references, a general description of the project's scope, and the value achieved by the referenced customers. They can testify to the service quality of the Vendors.

11.7 RFP Evaluation

The baseline for successful RFP evaluation is the evaluation criteria that determine the effectiveness with which you can compare and evaluate all the proposals received.

There are many ways to implement the evaluation criteria:

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

- Directly matching the compliance statement between the RFP requirements statements and all Vendors' proposals. Next, compare all the mandatory requirements with those Vendors who can comply fully and those with alternatives, and drill into further details if required to determine the most suitable Vendor.
- Establish a scoring system for each section of your RFP. For example, it can be based on a weighted system related to the degree of importance. Then, you assign each section to consider your comfort level with the vendor's response to your requirements.

In the following sections, we will look into details of mandatory portions you must be satisfied with before accepting the vendor's proposal and recommending it to the management for approval.

11.7.1 Legal Requirements

Check and confirm that the vendors accept all mandatory legal requirements. If there are deviations, you have to decide whether they are acceptable and present minimum risks to your organization. At the same time, ensure the compliance and level of liquidity damages are sufficient to address the level of commitment to the vendor in delivering the plan.

11.7.2 Business and Technical Requirements

Ensure all proposed hardware, software, and network equipment are similar to what you requested in the RFP. If not, provide equivalent functions and capacity to meet expected RTO and RPO requirements to address your business needs.

The DR delivery methodology is essential and critical to ensuring the DR scope and objectives can be met. Thus, thoroughly check and confirm how the vendor intends to manage and deliver the expected services using this methodology.

11.7.3 Qualification

For any DR Planning project, the experience of the Organization DR Coordinator from the vendor is the key driving force towards the successful delivery of the project; likewise, the technical expertise. To react to unforeseen circumstances, ensure replacements are available quickly. This is to minimize the impact and delays to the delivery schedules. You have to examine the qualifications that the vendor will deploy to deliver your project. If any individuals are unacceptable, immediately inform the vendor and request a replacement.

Although checking the references provided by the Vendors is very useful for verifying the Vendor's performance and capability. However, you must remember that the Vendors will not give a customer's reference that will provide adverse views on their organization and services. So, you must also check with your peers or network to determine the Vendors' quality.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Anyway, we would like to provide some key questions that you may want to verify with the references provided by the Vendor or through your personal or business contacts.

- Were they satisfied with the work done by the Vendor?
- Was it completed on time and within budget?
- Was the staff provided competent and experienced?
- Did the vendor have enough backup and competent resources to serve as replacement staff?
- Was there any significant scope creep during the engagement?
- Was the vendor responsive to satisfying their needs?

11.7.4 Cost

Besides ensuring the proposed cost is reasonable and acceptable according to your RFP's requirements, check carefully to ensure there are no hidden costs. Once you have established that the price is final, make it clear to the vendor that this is the final cost mutually agreed on, and any associated costs not discussed will be absorbed by the vendor.

Some of the basic costs to consider during the evaluation process include:

- One-time engagement cost for establishing the DR Plan, setting up the structure, and verifying the workability of the backup sites and equipment
- Operational costs: the monthly subscription cost of the backup sites and equipment
- Testing costs: the cost of conducting a DR test
- DR activation costs: the cost of declaring a disaster
- Tape handling costs: the cost of collecting and sending backup tapes to the offsite storage
- Any facility extension costs: the cost of using the backup site for extending the usage is permitted by the vendor
- Any other cost for conducting awareness programs, briefing, revising of DR Plan, and so on

11.7.5 RFP Award

After negotiating and agreeing with all the scope, schedule, items, deliverables and pricing of the proposal with the most suitable Vendor, carry out the formal contract award with the Vendor upon your management's approval.

However, before you sign on the dotted line, be careful that all the following documents are included in the entire contract document:

- Updated mutually agreed RFP document
- Vendor's proposal document

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

- Communication exchanges document such as emails, faxes, letters, and minutes of meeting
- Presentation materials
- Benchmarking documentation (if any)
- Any other supplements

12 Plan Development



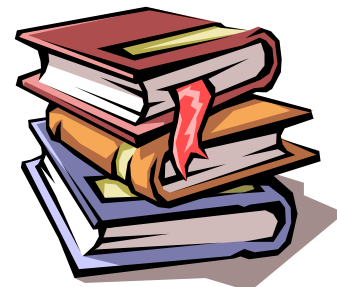
"All things are difficult before they are easy."

Anonymous

12.1 Overview

The DR Plan development process is a fundamental and essential step in establishing a comprehensive and extensive documentation set. This includes the complete business reaction, recovery and resumption procedures to counter any disaster events that may impact the business slightly or render a standstill to the business operation in its current operating environment.

As we all know, for a DR Plan to be comprehensive, it must contain the detailed roles and responsibilities of each of the DR team participants. It includes the inventory of all critical resources, procedures to activate the plan, recall of all DR teams, technical recovery steps to recover IT systems, verification steps to verify systems and vital data are recovered correctly, etc. In other words, it has to comprehensively capture all the steps and resources required to activate the DR Plan to operate comfortably using the adopted recovery strategy and finally return to regular operation at the original operation environment, whether in the existing location or a new location.



However, we should balance details with flexibility because the more detailed the plan is, the less scalable and versatile it will be. This will make the DR Plan inflexible in reflecting changes to the operating environment, especially when the current business environment is always the change regarding people, appointments, business direction, business strategy, business activities and operational business locations. Thus, a good DR Plan must be comprehensive, detailed, and adaptable to changes in business so that it is always in line with the current business environment.

This chapter will discuss the methodology for carrying out a complete DR Plan development process for DR practitioners. Also, we provide a sample DR Plan format in **Appendix F** for your reference. This document serves as a reference. You may have to tailor it to meet better the organization's specific system, operational, and organization requirements.

12.2 Planning Considerations for Plan Development

Before you start the DR Plan development process, you should develop a content outline for the DR Plan to serve as a general guide for developing detailed DR procedures. Thinking through the content outline will not only help you to organize your compilation of detailed recovery procedures, but it will also help you to:

- Determine the significant milestones and schedule to complete the plan.
- Identify any redundant processes and procedures that can be eliminated.
- Identify improvements to the coordination and interfaces between different teams and procedures.
- Identify the interdependency of DR teams and escalation flow.

Also, a standard documentation format needs to be established here to ensure look and feel consistency. For example, a consistent information presentation style, fonts, character sizes, section breaks, and paging will help all procedure writers to have a document frame to write on. The plan consolidator needs less effort to compile the overall DR Plan. The reviewer and management will have a clearer picture to vet and approve the DR Plan. Finally, the plan executor will be able to execute the plan correctly and effectively.

12.3 Disaster Recovery Teams

People are the key to executing and operating the recovery processes. Therefore, it must be appropriately selected, evaluated, trained, and re-trained to equip them with the correct mindset, skill sets, and tools to execute the DR Plan.

The DR teams are divided into various types of teams to take care of the individual systems and functions. The size of the team, name of the team and structure should be based on the DR requirements of the organization.

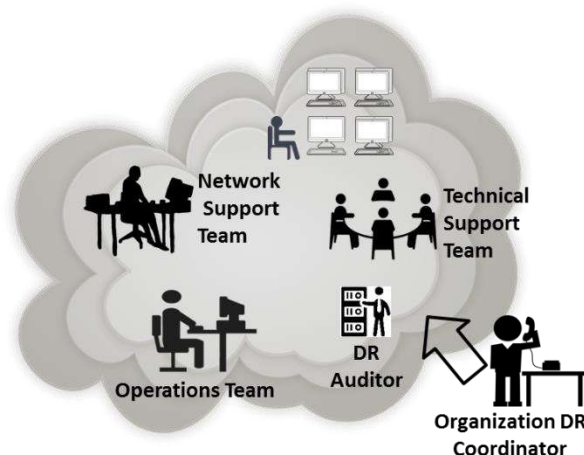


Figure 12-1: DR Team

12.3.1 DR Management Team

The Recovery Management team includes:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Recovery Manager (Usually the Organization DR Coordinator)
- Facilities Coordinator
- Technical Coordinator
- Administrative Coordinator
- Network Coordinator
- Applications Coordinator
- Computer Operations Coordinator

12.3.2 Business Recovery Teams (Non-IT)

Some key business recovery teams include the following:

- Executive Management Team
- Business Recovery Team
- Business Unit Recovery Team
- Damage Assessment Team
- Facility Support Team
- Administrative Support Team
- Logistics Support Team
- Transportation and Relocation Team
- User Support Team
- Media Relations Team
- Legal Affairs Team
- Physical/Personal Security Team
- Human Resources Team
- Procurement (Equipment and Supplies) Team
- Marketing and Customer Relations team

12.3.3 Disaster Recovery Teams (IT)

- The DR team includes the following:
- Computer Recovery Team
- Computer Backup Team
- Offsite Storage Team
- Software Recovery Team
- Communication Team

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

- Applications Team
- Computer Restoration Team
- Systems Software Team
- Network Operations Recovery Team
- Database Recovery Team
- Application Recovery Team(s)
- Hardware Salvage Team

12.3.4 Staff Selection Criteria

Staff selection criteria for the recovery teams should be based on:

- Skill-sets and business knowledge. Ideally, teams should be staffed with the personnel responsible for the same or similar operations under normal conditions. For example, Server Recovery Team members should include server administrators.
- The team's staffing and sizing must be optimized and remain viable, even if some members are unavailable to respond.
- Team members' alternation is one of the ways to address staff unavailability issues. Thus, team members must be familiar with other teams' goals and procedures to facilitate inter-team coordination.
- The team leader must be identified to direct overall team operations. Thus, they must be well-equipped with the knowledge, macro viewing capability, and a firm nature to be responsible for disseminating information to team members and approving any decision made within the team.

The DR Management Team is necessary for providing overall guidance following a major system disruption or emergency. The team is usually led by the Chief Information Officer (CIO) or someone with the authority to make decisions regarding spending levels, acceptable risk, and inter-organization coordination. Thus, the staff selected to be in the team must be:

- Able and capable of making a management decision on activating the DR Plan and supervising the execution of DR operations.
- Capable of facilitating communication among other teams and supervising plan tests and exercises.

Thus, when put into the correct position in the DR organisation structure, the right personnel with the proper attitude, capability, and skill-sets will ensure the correct execution of the DR Plan and achieve successful results as intended in the DR Plan.

12.4 Disaster Recovery Life Cycle

The main processes that form the complete DR Life Cycle encompass the following: a graphical workflow is also shown in Figure 9.2. Sometimes, this 6 Rs' is called the DR Life Cycle.

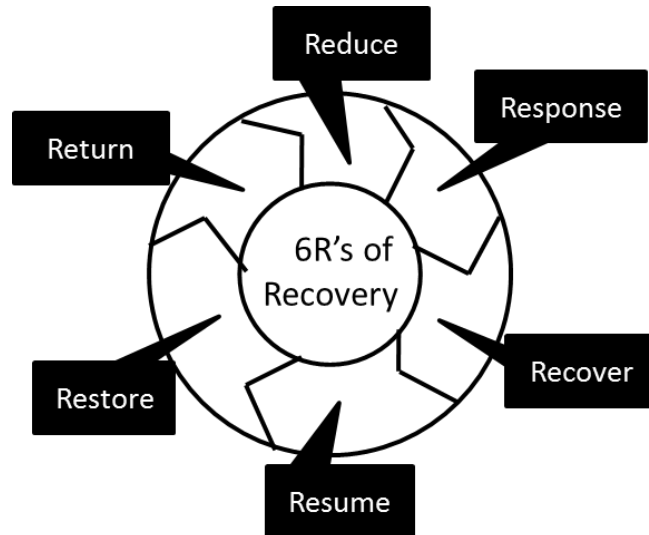


Figure 12-2: The 6 R's of DR Planning or DR Life Cycle

12.5 Components of a DR Life Cycle

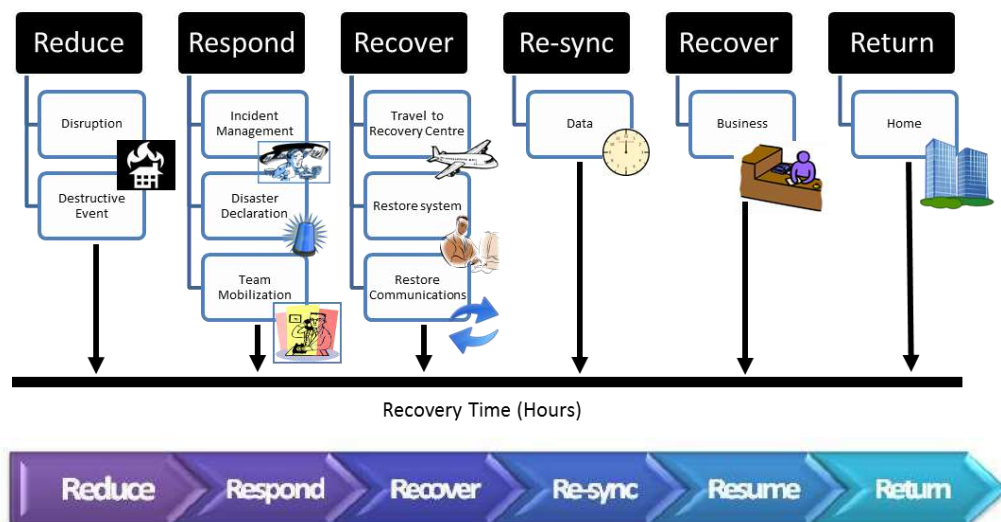


Figure 12-3: The Components of 6 R's within the DR Life Cycle

In addition, to Figure 12-3, these are the additional elements of the DR Plan. It should address the main areas:

12.5.1 Reduce

- Minimize, avoid or prevent the threats from occurring
- Prepare and exercise the DR plan

12.5.2 Response

- Detection: Detect a disaster event when it happens
- Notification: Notify the core DR team for initial assessments and verify whether a disaster has happened
- Damage Assessment: Assess the degree of damages done and decide on activation of the DR Plan
- Plan Activation: Activate the execution of the DR Plan
- Disaster Declaration:
 - Upon the decision to declare a disaster, the Disaster Declaration Officer will contact the recovery centre to declare the disaster
 - Check and confirm subscribed resources are made available
 - Activate specialized DR Team to be on-site and on standby
 - Confirm the time to access the recovery centre
- Team Mobilization:
 - Notification Call-Tree
 - Activate all team members to assemble at the designated assembly centre or alternate sites
 - Retrieve vital records from offsite storage
 - Activate key support vendors
 - Inform relevant parties

12.5.3 Recover

- Execute the recovery procedures and recover the business operation at a temporary site
- Travel to Recovery Centre:
 - Ensure that all team members need to be familiar with the location of the recovery centre
 - Consider the validity of travel documents and work permit or VISA to enter another country for support to overseas offices

12.5.4 Re-sync

- Re-synchronize Data
- Input data captured during manual business operations
- Perform audit check of data entered

12.5.5 Resume

- Test critical components of each application as per the DR Plan
- Verify that the correct data are restored by the Development or Application team
- Perform an audit on the readiness & integrity of data & security
- Authorize data to be released for production

12.5.6 Return

- Reconstruct the original site or acquire a new permanent site to return to the normal business operations
- Prepare primary site
- Equipment replacement or relocation
- Re-establish telecommunication
- Restore systems, networks, and applications.
- Conduct a parallel run to ensure the system at the primary site is stabilized
- Before cutover to the primary site from the recovery centre,
- Review of IT ends users and auditors
- Request the recovery centre to standby for at least one day after the cutover to serve as the backup

12.6 Timing of DR Life Cycle

This is the duration or estimated timing for the DR life cycle.

- **Reduce** - the period before the disaster
- **Response** - the hours and days immediately following the disaster
- **Recover** - the period from the occurrence of the disaster until temporary operations are restored
- **Re-sync** - the re-synchronization of data for all the systems
- **Resume** - the resumption of business functions and operations as the systems are gradually made available
- **Return** - the time when operations return to normal

12.7 General Information

In this section of the DR Plan, the purpose is to present the background on the overall DR Plan to aid the reader in understanding why, when and how to leverage the plan to execute the DR activities. A sample table of content can be found in **Appendix E**.

This section will generally cover the purpose, scope, authorities/references, and record of plan changes over time of this DR Plan. It will also orient the reader through the overall plan organization, so the reader can easily navigate the plan. Finally, it will also direct the reader to the type and location of information that needs to be referenced or related to this DR Plan. We will elaborate on some details of these main pointers in the following sub-sections.

12.7.1 Purpose

Give a purpose statement to establish the reason for developing this DR Plan and define the plan objectives to give the reader a heads-up on what information will be presented.

12.7.2 Scope

Scope the situations or conditions that this DR Plan will cover so that the reader knows what the DR Plan will address. Examples of possible scopes of the DR Plan that you may wish to consider are:

- Address only critical IT systems that are needed to support critical business operations in Sales, Production, Delivery, and Finance
- Address IT systems and also the locations where these IT systems are installed in the system is distributed among multiple locations
- Address short-term disruptions that are expected to last fewer than four hours, or it may not address catastrophic events that destroy the IT facility

Remember to state any assumptions you have made for the plan. Otherwise, these unwritten assumptions can turn the whole plan non-workable. However, assumptions are not intended to substitute or replace the need for thorough planning in DR. Thus, do not make an impractical assumption such as the DR Plan only addresses disruptions during business hours. A DR plan is meant to address all disastrous situations at any time because disasters do not happen only during business hours.

12.7.3 Information Classification

The DR Plan contains all critical details about the organization's IT infrastructure, systems and processes needed to support the operations of the business activities. Therefore, there is a need to control the plan distribution to safeguard the sensitivity of the information contained in the DR Plan. Also, a strict policy and penalty statement must be established to make all DR personnel aware of this DR Plan's safeguards.

12.7.4 History of Changes

The DR Plan is a “living” document, and keeping it up-to-date and in line with the existing operation and the environment is critical. Thus, there is a need to keep track of the details of the changes that have been done, the date and the person who updated the plan. This is recorded on the front of the plan to inform the reader of the DR Plan and what has been changed.

12.7.5 Organization Chart

There should be a detailed description of the organization structure for the DR teams using only specific DR roles, not names of individuals. Doing so will reduce confusion and minimize the hassle of changing the DR Plan whenever there is a personnel turnover.

This DR organization structure should aim to provide:

- An overview of team member roles and responsibilities in a DR situation
- Specific response and recovery roles during DR Plan activation
- Coordination mechanisms and requirements among the teams

12.7.6 Overview of DR Plan

The provision of an overview and brief description of all system architecture, location(s), and any other critical technical considerations addressed in the DR Plan will give the reader a feel for the scale of the plan's coverage. If possible, including an IT architecture diagram will be helpful.

12.8 Reduction Stage

This stage is usually not documented in the DR Plan. However, it forms part of the risk assessment plan.

12.9 Respond Stage

In the Notification/Activation stage of the plan development process, we will look into the actions that need to be taken once a system disruption or emergency has been detected or disastrous. The DR activities included in this phase are disaster detection, call-tree notification, damage assessment, and DR activation. At the end of the Notification/Activation stage, all DR participants or appointment holders will be prepared to perform DR activities to recover and restore system functions temporarily.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

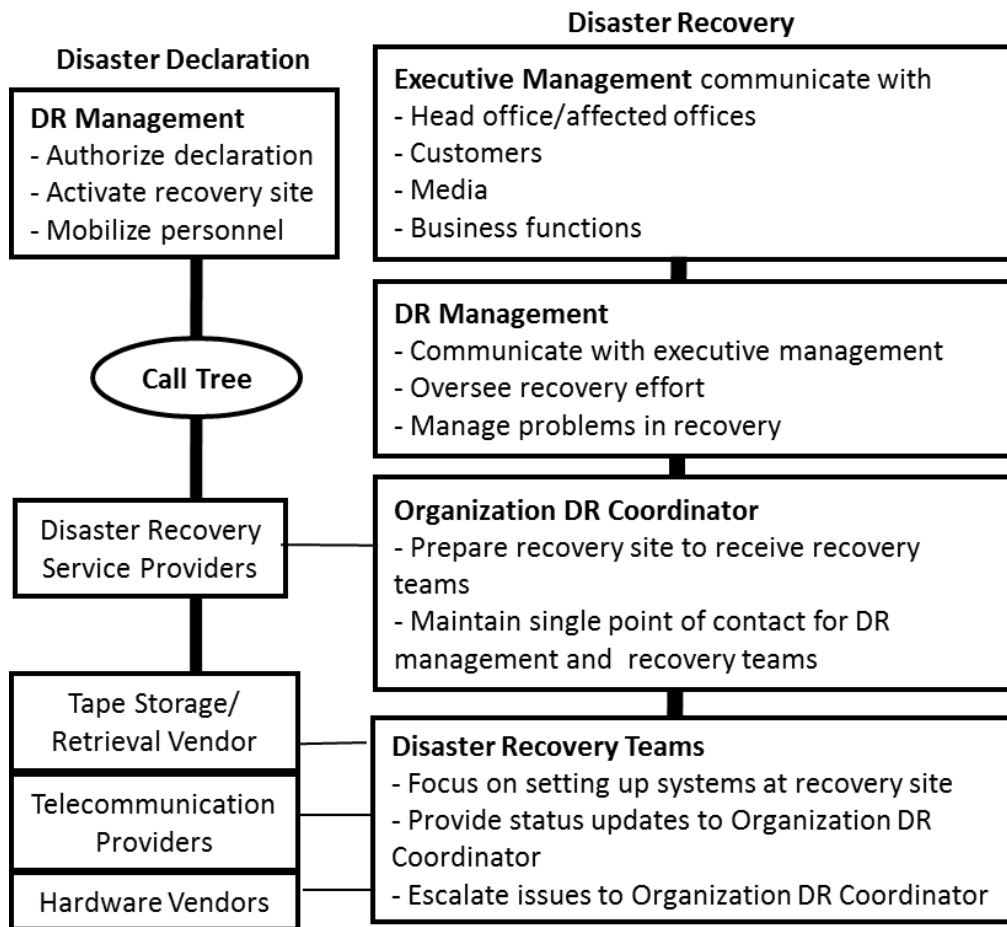


Figure 12-4: Initiating the Communication Process

12.9.1 Notification Procedures

A disaster event may occur with or without prior notice. For example, advanced notice is often given when an imminent hurricane affects an area. Pre-emptive warnings that a computer virus is expected to hit computer systems on or by a specific date is another example.

However, there may be no forewarning for equipment failure, criminal acts or terrorist attacks. Notification procedures must be documented in the plan. Describe the procedures and the methods used to notify recovery personnel during business and non-business hours. Prompt notification is essential. In some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

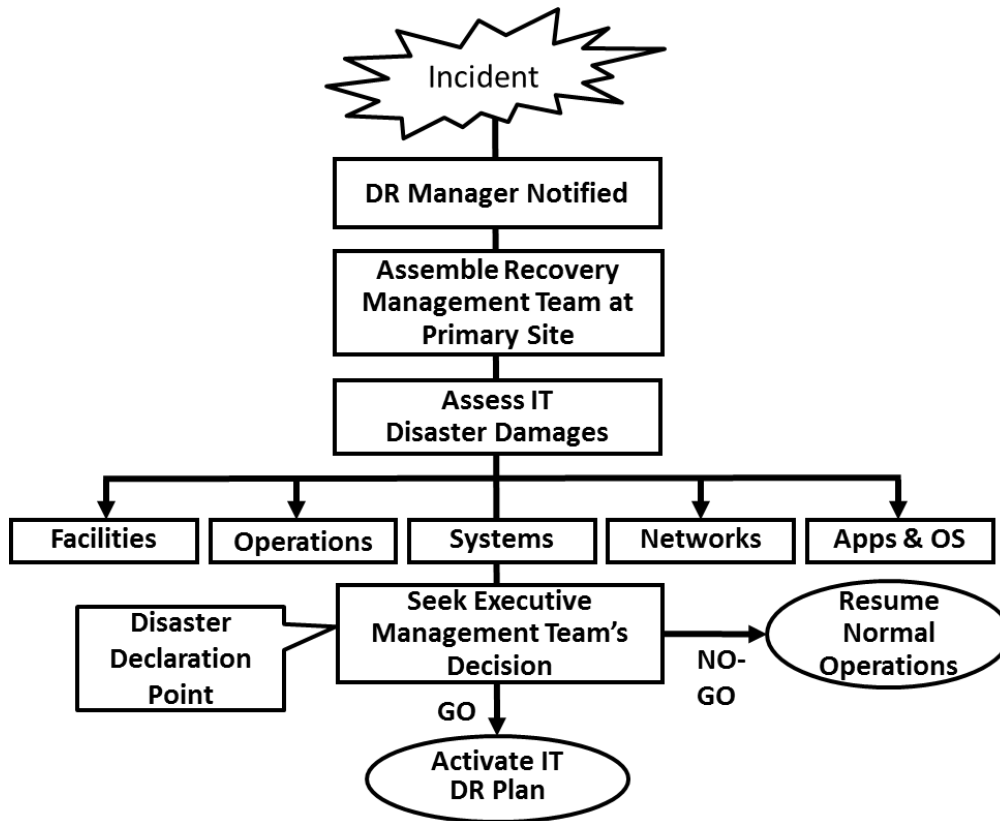


Figure 12-5: Disaster Response Flowchart

Following a disaster event, the Damage Assessment Team must be notified immediately. This team will be required to assess the status of the situation and advise Executive Management to allow management to make appropriate decisions. When the damage assessment is complete, the proper recovery and support teams should be notified.

Notifications can be accomplished through various methods, including telephone, pager, work or personal electronic mail, or cell phone. Notification tools effective during widespread disasters include radio and television announcements and websites. Procedures and processes to provide information to personnel who cannot be contacted must also be defined. Notification procedures should be documented clearly in the DR Plan. A typical notification method is a call tree. This technique involves assigning notification duties to specific individuals who are responsible for notifying other recovery personnel.

Both primary and alternate contact methods must be listed in the call tree, and procedures to be followed if an individual cannot be contacted. A sample notification call tree is shown in Figure 9.5.

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

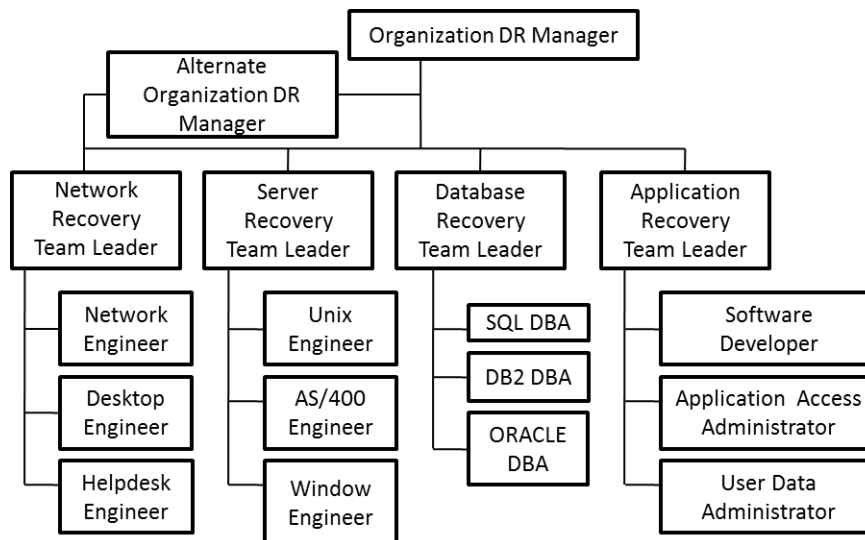


Figure 12-6: Sample Notification Call Tree

12.9.2 Notification Contact List

On a notification contact list, the following items must be made available and kept up-to-date and accurate so that all DR team members can be notified and activated promptly during an emergency.

- DR team position
- Name of staff members
- Home telephone number(s)
- Workplace telephone number(s)
- Mobile or cellular phone number(s)
- Email addresses
- Home addresses

The notification process should not be limited to within the organization. It should extend to all external organizations, interconnected system partners, vendors, and customers that may be adversely affected if they are unaware of the situation. Some of these external organizations or affiliated system partners or vendors include government bodies such as power utility boards, and email outsources service providers, telecommunication linkages providers, off-site storage service providers, etc.

The type of information to be communicated to the DR team should be short, precise, and to the point so that the information receiver will immediately know the next step, they should carry out directly. The basic information to be communicated must, at least, include the following:

- Nature of the incident that has occurred
- Any loss of life or injuries
- Any known damage estimates

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Response and recovery details
- Where and when to convene for briefing or further response instructions
- Instructions to prepare for relocation for the estimated period
- Instructions to complete notifications using the call tree (if applicable)

Time	Typical Recovery Time Needed
Start Time	Disaster occurred
15 mins	Notification of disaster by building security
10 mins	Organization BCM and DR coordinators inform the DR management team
10 mins	Assessment of disaster situation
10 mins	Activation of disaster to Recovery Centre
4 hours	Recovery Centre preparation
2 to 3 hours	Mobilization of DR team to Recovery Centre
2 to 3 hours	Activation and delivery of vital records from offsite to the Recovery Centre

Time	Typical Recovery Time Needed
30 mins	Assembly and staff briefing at Recovery Centre
10 to 15 hours	Recovery of services and communications
2 hours	Application testing
1 hour	Data synchronizing and audit
15 mins	Online - communication establishment

Figure 12-7: Sample DR Timing and Sequence

12.9.3 Damage Assessment

Before the decision to activate the DR Plan, a damage assessment has to be carried out to assess the degree of the damage and whether recovery at the original site or equipment is possible. Damage assessment is key to deciding on DR Plan activation. The faster a decision can be made, the quicker the recovery process can be put in place and

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

the sooner the business can be put back into operation. Thus, in all situations where circumstances permit, the Damage Assessment Team will be among the earliest to be notified of the incident and arrive at the damage scene to carry out the assessment.

Always focus on personal safety as the priority in any damage assessment procedure. Then focus on the following essential areas to derive a recommendation to the management on whether there is a need to activate the DR Plan:

- Cause of the emergency or disruption
- Potential for additional disruptions or damage
- The area affected by the emergency
- Status of physical infrastructure (e.g., the structural integrity of the computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning [HVAC])
- Inventory and functional status of IT equipment (e.g., fully functional, partially functional and non-functional)
- Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact and electrical surge)
- Items to be replaced (hardware, software, firmware and supporting materials)
- Estimated time to restore normal services

12.9.4 Plan Activation

The DR Plan should be activated only when the damage assessment indicates that one or more of the activation criteria for that system are met. If an activation criterion is completed, the Organization DR Coordinator should then advise the Executive Management to activate the plan. However, there is no hard and fast rule for DR Plan activation. Each organisation's activation criteria are unique, and you may state them clearly in your organization's DR Plan policy statement.

Some of the criteria you may consider for DR Plan activation are as follows:

- Safety of personnel and extent of damage to the facility
- The extent of damage to the system (physical, operational or cost)
- Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset)
- Anticipated duration of the disruption

Once the activation of the DR Plan is declared or sometimes referred to as disaster declaration, the notification process to recall all the DR teams listed in the DR recovery process will also be activated. The DR teams will follow the recovery sequences.

12.10 Re-sync and Recovery Stages

The recovery operations will begin after the DR Plan has been activated, a damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.

The recovery activities' primary focus is restoring temporary IT processing capabilities. Thus, the expected result for the recovery phase is that all critical IT systems will be operational and perform the functions designated in the DR Plan.

12.10.1 Sequence of Recovery Activities

The recovery sequence is a key factor in determining the success or failure of the recovery plan. Thus, all recovery procedures should be written in a sequential and step-by-step format to restore the system components logically. It must also reflect all expected interdependencies and the system's allowable outage time to avoid significant impacts on related systems and their application. For example:

- If a LAN is being recovered after a disruption, the most critical servers should be recovered before other, less critical devices, such as printers.
- Similarly, procedures should first address operating system restoration and verification before recovering the application and its data to recover an application server.
- Certain materials must be transferred or procured if conditions require the system to be recovered at an alternate site. Procedures should also designate the appropriate team or team members to coordinate the shipment of equipment, data, and vital records to be done before the recovery actions can be executed.

Some of the pointers for coordination between recovery procedures should also include instructions to coordinate with other teams when certain situations occur:

- An action is not completed within the expected time frame
- A critical step has been completed
- Item(s) must be procured
- Other system-specific concerns

12.10.2 Recovery Procedures

To facilitate the recovery operations, detailed procedures to restore all the IT systems and their components must be clearly written in such a way that it is easy to read and understand and will not create any doubt when read by a third person who is not involved in the development of the plan. This is critical as the person who needs to carry out the recovery process may not be you or the person who wrote the DR plan.

Some of the key pointers for carrying out the development of these detailed procedures are:

- Make the right recovery team do the writing.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- DR notifying procedures to inform all internal and external business partners associated with the system
- Procedures for take-over recovery site's hardware, network, workstations and other accessories required for the IT systems recovery
- Procedures to acquire, deliver and install necessary hardware components
- Procedures to recall, collect and recover data from backup tapes or media
- Procedures to restore and test the functionality of the critical operating system, application software, and patches
- Procedures to restore and verify recovered system data and user data
- Procedures to carry out system functionalities tests
- Procedures to connect, test and verify the systems' connectivity with external networks or interfaces with other remote systems
- Procedures to inform and assist remote users in connecting to the recovered systems

A key guideline to writing recovery procedures is a straightforward and step-by-step style to avoid confusion or guessing during a disaster. An unclear and confusing procedure will cause a disaster. Therefore, a checklist-style recovery procedure is ideal as it is easy to read, straight to the point, and step-by-step, with one sentence for one task.

For example, take a look at a sample Unix Server Recovery Checklist:

S/No	Procedures	Time Taken
1	Identify the version of the Operating System and the patches that need to be applied from the Inventory List <u>Page X of 7</u> in <u>Appendix XX</u> of the DR Plan.	
2	Identify the tape number using a tape log book.	
3	If the tape is not in a tape library, request a tape from the offsite storage team leader; fill out a request with the appropriate authorizing signature.	
4	When the tape is received from the offsite storage team leader, log the date and time	
5	Place tape into the drive and begin the recovery process	
6	When the file is recovered, notify Unix Server Recovery Team Leader	

Figure 12-8: Sample DR Procedures

This book will not provide specific recovery procedures as there are many different systems (IBM, HP, Sun, Dell), configurations, operating software, databases, and

applications. It will be pervasive under the scope to cover them all. However, some sample recovery considerations for some IT system types are enclosed in Chapter 13 for reference.

12.11 Return Stage

After you have successfully recovered and gained full operational capabilities of the recovered systems at your recovery site(s), it is time to start the reconstruction process at the original site. If the original site is not recoverable, it is time to start sourcing, acquiring and preparing a new site to migrate your business operations from the temporary recovery site(s) back to your permanent business operation site.

The steps that you need to document in the DR Plan should include some of the following main steps involved in the “back-to-home” phase:

12.11.1 Original Site is Beyond Recovery

A new permanent site must be sourced and acquired if your original site is beyond recovery. It would help if you listed a checklist to pinpoint the key considerations and factors to look out for when sourcing the new site. Some of these critical considerations may include:

- Preferred locations because they must be near your corporate office, utility suppliers, and logistic suppliers
- Specific utility requirements, such as telecommunication, electric power, air-conditioners and water supplies
- Specific technical requirements for central versus own controllable air-conditioning units, power supplies units, backup power generators, fire detection and suppression systems and security access system
- Specific infrastructure requirements, raised floors, fire-rated walls, multiple access controls to many different locations for safekeeping your IT equipment and documents
- Any restrictions to alternation of building walls, electrical distribution design and setting up of in-house air-conditioners, operation hours of air-conditioning to a section of the office
- The kind of business operations your neighbour (s) are in and whether they will induce risks to your business operations. For example, do not select a place that is directly for a restaurant operator to house your servers

12.11.2 Recovering from a Damaged Original Site

If you are recovering from a damaged original site, including a checklist to ensure all the undesirable items are removed, proper clean-up has been carried out, and all necessary utilities, detection systems, and network infrastructure are set up accordingly.

12.11.3 Restoration

When the original site is restored, or a new permanent site is constructed to the operationally ready level to support the IT systems and its normal business processes, a series of take-over tests must be carried out to verify:

- Adequate readiness and stability of all essential utility services, such as both primary and backup electrical power supplies, air-conditioners, telecommunication linkages, and environmental controls
- Adequate and readiness of fire and water detection and suppression system(s)
- Operational readiness of security mechanisms such as electronic card keys, video cameras and scanners to safeguard the computing facilities
- Operational readiness of all internal network cablings and network equipment

12.11.4 Confirm the Operational Readiness of the Original Site

After confirming the operational readiness of your original site, the IT systems can now be transitioned back to the original or the new permanent site. The primary activities should be thought through carefully and documented in detail. Some of these key activities are as follows:

- Installing system hardware, software, and firmware in priority sequence. The documentation for installations is similar to the detailed restoration procedures for the DR centre
- Establishing connectivity and interfaces with network components and external systems
- Backing up operational data on the DR system and uploading it to the restored system
- Shutting down the DR system
- Declaring the original site is ready for operation and terminating DR operations
- Arranging and transporting all recovery personnel back to the original site
- Removing and relocating all sensitive materials at the DR alternate site

After all the key personnel are back and have started operation at the original site, you can consider the “back-to-home” phase to be successfully achieved.

12.12 Appendices for DR Plan

12.12.1 Criteria for Appendices

- The appendices of the DR Plan will cover details that you can easily detach for specific usage for specific people, information that changes quite frequently (like the contact list) and key information not contained in the main body of the plan. The guideline for including appendices to the DR Plan is that it must reflect at least one of the following:
 - Specific technical requirements for an IT system
 - Specific operational requirements for an IT system
 - Detailed management instructions or requirements for an IT system



12.12.2 Benefits of Appendices

Good sequencing of detailed and yet frequently changing DR information when put into appendices will help you in:

- Easier management and keeping the DR Plan up-to-date
- Reducing paper usage as there will be a lesser need to re-print the entire DR Plan for distribution
- A more systematic way of managing the distribution and collection of DR Plan updates from all DR team members

12.12.3 Common Appendices Items

Some of the common items that you may want to cut out from the primary DR Plan and insert as appendices are:

- Contact information for key decision-makers, critical resource providers and also the people who execute the DR Plan, such as Executive Management, DR Teams, key suppliers, system vendors, offsite storage vendors, emergency authorities and building management
- SLAs, contracts and agreements with vendors who are required to support the recovery and operation of the DR site and facilities. Some examples are the hot-site contract document, off-site storage agreement and agreement for providing specific hardware with a specific delivery time
- Hot-site or recovery site address, location map, transport availability, contact numbers, activation sequence, codes or passwords, etc.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Equipment and system inventory lists that cover all details such as manufacturer, model, and make, version number, license number, serial number, and quantity, for all hardware components, firmware versions, operating systems, application systems and other resources that are required to support the operation
- BIA document that contains valuable information about the interrelationships, risks, prioritization and impacts on each element of the system

12.13 Conclusion

It is important to note that a DR plan is a “living” document refined over several iterations. This document needs to be updated over time, no matter how well it was developed initially. Do not be discouraged, as most plans will fail during the execution initially, but the key is to continue improving the DR plan to work when needed.

13 Testing and Exercising



"DR Plan that is not tested or testing without a plan is equally disastrous to an organization."

Goh, Moh Heng

13.1 Overview

In IT, there are two key groups of users of the DR Plan. They are the business owners and the IT service providers. Thus, they have different requirements for testing the DR Plan. Therefore, the Organization DR Coordinator needs to understand these different expectations so you can effectively manage the complete DR testing lifecycle (Goh, 2006).

The business owner's objective for testing the DR plan is to evaluate whether or not the DR Plan can restore one or more business-critical processes to functionality within the defined RTO and RPO. As a result, the DR test provides a high level of assurance for business owners with minimal associated costs and no disruption of services.

From the IT services providers' angle, DR testing will assist them in verifying that the DR Plan is current and has catered for all recovery needs regarding hardware, software, regulatory and legal implications, risk analysis of newly identified threats, vulnerabilities, and safeguards.

In general, DR Plan needs to be tested to ensure that the business can continue the critical business processes in a disaster. The Recovery procedures must be executable and accurate. Another benefit of testing the plan is training the personnel responsible for executing the DR Plan. The vital issue is not whether the test is successful and without problems but whether the test results and problems encountered are reviewed and used to update or revise the current DR Plan procedures.

DR Plan testing (Goh, 2006) involves mobilizing a support team from technology organizations, vendors, and users. Depending on the testing methodology, testing is usually carried out during weekends, outside normal office hours. A DR test can be costly and, therefore, requires justification. These are some rationales that can be considered:

- Confirm the validity of the DR Plan
- Conform to corporate policy, legal or regulatory requirements
- Review and demonstrate DR capability to meet business requirements
- Identify any shortcoming

- Fine-tune and improve recovery procedures
- Rehearse

DR Plan testing can be broadly categorized into the following three broad stages:

- Pre-test planning
- DR test execution
- Post-test review and documentation

13.2 Pre-test Planning Activities

Pre-test planning includes defining the requirements, designing the test approach, test scenarios, key success measurements and developing a detailed activity plan.

13.3 Define Scope and Objectives for Test

Defining the objectives and scope of the DR test is to ensure the DR Plan is adequately and accurately tested. A clearly defined statement also provides that all participating teams understand the scope and objective of the test. For example, a DR test objective is to test the recovery procedures simulating a total data centre site failure.

The scope of the test can cover both online and batch services that support critical business processes, which are identified during Business Impact Analysis. The scope of the test can also be extended to include call tree testing, testing mobilization of the recovery team, and testing the disaster notification and invocation procedures. In recent years, BCM testing (ISACA, 2012) should include services provided by cloud vendors.

13.4 Design Test Scenario

Test scenarios can vary from simulating a data centre site failure or a unit test affecting a specific system or infrastructure failure.

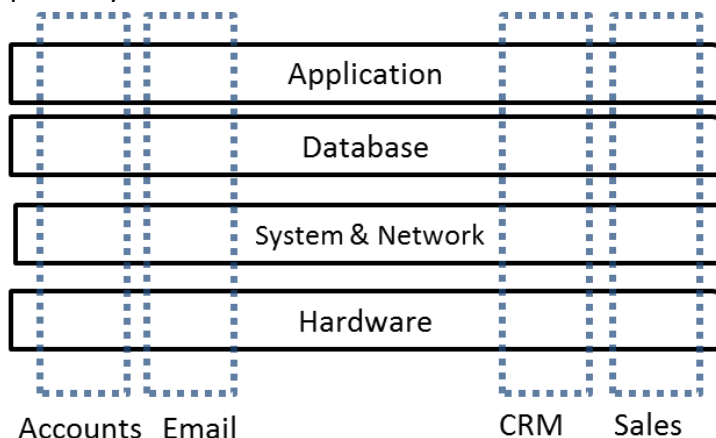


Figure 13-1: Test Different levels and Functions

13.5 DR Plan Test Cycle

Several test approaches can be considered:

13.5.1 Checklist Test

Checklist testing is inexpensive but provides a good backbone for the DR testing cycle. A checklist test is usually carried out by dividing a business process into areas of responsibility and then grouping the DR teams involved in the respective areas to run through the checklist required for recovering this specific area of operation.



This test approach is particularly suitable for validating the following areas:

- Call Tree list
- Key recovery procedures, such as AS400 server recovery steps
- Completeness and correctness of hardware and software inventory list
- Completeness and correctness of tape backup libraries

13.5.2 Paper Test

A paper test reviews the DR procedures and other response documentation, such as a contact list.

13.5.3 Walkthrough Test

A walkthrough test is a classroom-based walkthrough with the recovery team members of the scenarios and action steps documented in the DR Plan to:

- Confirm plan effectiveness
- Identify gaps and bottlenecks between procedures and processes
- Identify weaknesses in the DR Plan

This is a practical test and less intrusive to normal operations. Still, it provides the opportunity to involve a larger group of users and allows you to draw upon a correspondingly increased pool of knowledge and experiences.

13.5.4 Phase Approach or Unit Test

The “Phase approach” or “unit test” tests the recovery of a particular platform or infrastructure. For example, if changes invalidate the DR Plan, the procedures must be revised and the DR Plan re-validated. A phase approach test or unit test can be applied to optimize the scope of the test to the affected or changed environment.

13.5.5 Cutover or Parallel Test

A Cutover Test prepares and ensures that the recovery systems can support critical business functions. In contrast, a Parallel Test requires testing the processing functionality at the alternate site.

A disaster is simulated so normal operations will not be interrupted. Usually, hardware, software, communication networks, recovery procedures, recall backup tapes, the order of mandatory supplies and forms, and alternate site processing will be activated during a simulation test. Under this test, historical transactions such as the previous business day's transactions are processed against the preceding day's backup files at the alternate site. Therefore, all reports produced at the alternate site for the current business date should agree with those made at the main office.



The test should be considered in advance and only implemented after the previous checklist, and walk-through tests have been validated.

13.5.6 Full Interruption Test

The full Interruption test simulates a vital disaster scenario involving the DR Plan's invocation. However, the resource commitments to carry out such tests are higher and, therefore, more costly. In addition, the test can be disruptive to normal operations. Consequently, it is important to be cautious and minimize the impact on normal operations.

13.6 Design the Key Success Measurement for the Test

What constitutes a successful DR test, and what are the measures to quantify a DR test? First, the key success measurements should be quantifiable. For instance, a successful DR test demonstrates the capability of recovery within 6 hours of all critical services identified during BIA. In addition, the test is 100% certified by all business units.

13.7 Design of Other Key Test Components

Apart from designing the test approaches, scenarios, and critical success measurements, a DR test plan should also address the following components:

- Identify the DR test team
- Document a list of assumptions made
- Identify the limitations of the test
- Identify resource requirements/ logistics and budget
- Pre-test validation of users' requirement

- Identify inter-dependency requirement
- Identify risks and implement control to mitigate the risk to normal operation in a DR test
- Develop a detailed activity plan
- Obtain management approval of the test and management sign-off of the test results
- Pre-tests briefing

A sample DR test Check and A sample DR test design template can be found in **Appendix K** and **Appendix L**, respectively.

13.8 Content of a Finalized Test Plan

After going through all the above activities, you should achieve a complete test plan equipped with all the following major components for carrying out the DR test.

Draw a schedule that captures all the test planning sessions, pre-test technical reviews, user briefings, and post-test debriefs.

Have an introduction that captures the Scope, Test Objectives, Test Scenario, Test Assumptions, Dependencies and Success Criteria, and exclusion (if any).

Test team details.

- Test timeline planned start and stop time of each test task and critical test checkpoints
- Critical test checkpoints, activity, party, and recommendation
- Test Problem Logs that capture any problems encountered before and during the test and any deviations from the test plan were done

13.8.1 Execution of Test

The DR Plan test execution phase will focus on testing the recovery procedures' reliability, efficiency, and accuracy. The Organization DR Coordinator oversees the entire event, which involves controlling the test activities, managing users testing, managing problems and ensuring no interruption to normal operations.

A DR test should invoke the Emergency Response and Operation practice in the DR Plan as a best practice. Emergency response and operation define the organization and operations in response to a major incident to stabilize the situation.

13.8.2 Managing Test Activities in Test

Track all scheduled activities as documented in the test plan. This ensures that scheduled activities are executed promptly to meet the recovery time objective. Be aware of any delay that could jeopardize the test or impact normal operations. A good DR test activity plan should include relevant control checkpoints to assess the situation and monitor the event.

13.8.3 Managing Users in DR Test

The challenge is to ensure users testing is carried out timely and thoroughly. Users should prepare the test scripts to be performed during the test. The Organization DR Coordinator should conduct users briefing to advise users of their roles and the communications, coordination and problem-reporting procedures.

13.8.4 Managing Problems in Test

In most test situations, the DR environment has to return to the service provider or for other internal use. Problems encountered during the test should be resolved within the limited test window. Therefore, users should make every effort to report problems promptly so that investigation and remedy can be quickly taken during the test window.

13.8.5 Managing Risk to Normal Operations in Test

Interfaces to external systems, automated recovery scripts to recovery systems or linkages are exposed to risks of DR transactions sent to external parties. Similarly, in the simulated DR test scenario, users' login to normal production instead of the DR system can damage the business. Therefore, pre-test risk analysis should be carried out to eliminate such risks.

13.9 Post-test Review and Documentation

After completing the DR test, the next phase is to document the test results, study and analyze problems encountered, review recovery procedures, identify key lessons learned, and update the DR Plan.

13.9.1 Consider Major Tasks

Some of the major tasks to be considered during the post-test review should include:

- Consolidate users' test results and recovery team feedback
- Compile key success measurements and metrics
- Perform root cause analysis on problem encountered
- Follow up on permanent fix to prevent the recurrence of the same problem in future
- Review recovery procedures and identify the opportunity for improvement
- Document key lesson learned, which includes positive and negative feedback from the DR test
- Retain necessary logs and evidence for audit
- Update procedures and prepare DR Test report
- Update Users and Management

13.9.2 Guidelines for Establishing the Post-test Review Document

The Post-test review document aims to identify problem areas encountered during the DR test and establish the required improvements to the DR Plan. Some of the items that are needed to be set up in the review document will include:

- Summary of the overall test results
- Timeline planned tasks with start and end time compared to the actual tasks executed with actual start and end time committed
- Problems encountered, such as problem descriptions, resolution status, and resolution descriptions
- Observations
- Recommendations for areas to be tested or re-tested for the next DR test

14 Program Management



*"Expect the best, plan for the worst,
Moreover, prepare to be surprised."*

Denis Weitley

14.1 Overview

The DR Plan is a "living" document that must be adequately maintained to ensure reliability and accuracy. This is because any changes to the typical operating environments, such as systems, networks, utilities, applications and business environments, would invalidate the particular contents of the DR Plan. This includes the inventory list, contact list, recovery process, and procedures, and it renders the DR Plan useless.

Thus, effective change control and management procedure that ensure all the following areas are covered must be established and practised so that the DR plan is updated with the latest development in the organization, especially in the IT support field.

The appropriate evaluation of any change that could impact the DR Plan is done when the difference arises due to business re-direction, systems upgrades or enhancement, application upgrades, or new services.

The Organization DR Coordinator must be informed and made aware of any changes that impact the DR Plan. They will then realign the DR Plan to address the changes and test and re-test the updated DR Plan to ensure that it can still cover the business's recovery requirements in the new environment.

Also, a formal audit and review of the DR Plan should be conducted at least once a year to assess its readiness of the DR Plan. It is also to confirm that those changes that happened since the last review are captured in the DR Plan. The audit and review process should pay particular attention to configurations of recovery equipment to ensure that the required equipment is available to restore the business functionality as quickly and smoothly as possible

This chapter will go through the major topics of having an actual and effective DR Plan maintenance process (Goh, 2010b).

14.2 Major Considerations for Maintaining DR Plan

The major considerations for setting up the DR Plan maintenance processes are:

- Define clear accountability of individuals to maintain relevant procedures so that every individual within the DR team is responsible for keeping their section up-to-date with the setups in the existing working environment
- Ensure change control and management process that include evaluation of any impact on the DR Plan and tracking of appropriate updates are carried out accordingly
- Conduct regular DR tests to validate the reliability, accuracy and efficiency of the DR Plan
- Enforce periodical inspection and assessment programs to audit and review that all changes to the DR Plan are done according to the change control and management procedure and the DR Plan is updated with the latest information

DR Plans are distributed promptly, correctly and effectively to all the DR team and management when an update is done.

14.3 Plan Maintenance Process

For a DR Plan to be reliable and accurate, it must be up-to-date. Some guidelines are discussed in the following sections.

14.3.1 Define Clear Accountability of Individuals to Maintain Respective Procedures

The Organization DR Coordinator should be responsible for maintaining the master DR Plan. In addition, respective subject matter experts responsible for the maintenance of systems, networks, utility software, and applications should be accountable for maintaining the respective recovery procedures.

14.3.2 Change Management Process

The Change Management process is critical to the DR Plan. The organization should institute a mandate to evaluate the impact of changes to the DR Plan. These changes can be due to the new implementation, upgrade or maintenance. The organization should adopt a policy on changes that invalidate the DR Plan, its recovery procedures, and the revised DR Plan to be retested within a specific timeframe. The Organization DR Coordinator will need to be in the loop of such changes, especially in the following areas:

- Personnel changes
- Business Mission changes
- Business Priority changes
- Backup procedures

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Recovery procedures
- Facilities relocations or consolidations
- Software changes (operating system, application programs)
- Hardware changes (addition of new peripherals, upgrades to CPU, RAM, Hard disks)
- Communications Networks extensions, expansions or consolidations

14.3.3 Periodic Inspection and Assessment Programs

The periodic inspection and assessment programs ensure that the designed DR processes are followed and maintained up to date. In addition, independent review and testing of the plan will maintain its high quality and consistency.

Some typical periodic inspection and assessment programs to be considered are:

- Verify that all contact lists specified in the DR Plan are the latest
- Review the currency and the frequency of updates of the recovery procedures, hardware configuration information, system software, and network and application systems inventory
- Validate that the applications recovery priorities are established
- Validate that the DR requirement is included in the development life cycle
- Review periodically the backup arrangements made with suppliers and vendors
- Test the DR Plan regularly to ensure its functionality
- Evaluate the adequacy and effectiveness of the alternate recovery site for contingency needs when the alternate recovery site agreement expires

14.4 Plan Distribution Process

The DR Plan is a highly confidential document as it contains sensitive information on your entire network infrastructure and detailed configurations of all your servers and applications. At the same time, your DR Plan also recorded critical contacts of your organizations, business partners, and suppliers and the list of vital records. Thus, a proper document distribution and control access process must be established to ensure only people who need access to the DR Plan are given a copy.

For proper tracking and management of all copies of the distributed DR Plan, a distribution matrix that indicates who should receive copies of the DR Plan must be documented and updated as and when there are changes to this staff list. In general, a distribution list for the DR plan should include the following people:

- Executive Management
- Data Centre Management
- Computer Operations Management
- DR team members

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

- Internal Auditor
- DR Site Operator
- A copy at the DR location

Some good practices for organizing the DR Plan for easier management of distribution and collection are listed as follows:

- Assign a unique number to each copy of the DR Plan
- Link each numbered DR Plan with the staff who is holding it
- Print unique page number, version number, and date of update on every page of the DR Plan by Chapters or Sections
- Remove information that changes more frequently, such as hardware and software inventories and staff contact list, from the main DR Plan document and put them under appendices to the DR Plan
- If you are familiar with the documentation structure of the ISO 9000 documentation format, use it for the DR Plan

A good DR Plan distribution process is always to exchange the latest release of the DR Plan with the existing copy that the staff listed in your DR Plan distribution matrix is holding and destroy the old documents.

14.5 Make a Multi-Year Investment in Recovery

Finally, after obtaining accurate estimates for improving application recovery, you may plan for a multi-year investment that enhances the most critical applications in the first year and less-critical applications in subsequent years. Alternatively, you can use staged investments to improve recoverability incrementally.

15 Program Management: Awareness and Training



"What goes up slowly comes down fast."

Michael Baume

15.1 Overview

When a DR Plan is reckoned to be needed for the organization, awareness and training should be seriously considered and put into action to raise the awareness and understanding of all personnel in management to appreciate the benefits of having a DR Plan. This includes the negative impacts of not having one, the methodology for developing the DR Plan, the DR processes and procedures required, the skill sets needed to carry out our recovery works, etc. Well-trained personnel with a high level of awareness are critical in ensuring a successful recovery from a disaster situation.

Ironically, the importance of awareness and training (Goh, 2010b) is typically overlooked after a vast amount of time and resources have been spent building up the DR Plan. Consider this scenario in which an employee of the organization does not know how to use a fire extinguisher, or even worse, and they may not even be aware of the location of the extinguishers. A well-designed DR Plan can address the most significant reaction when a fire is detected in the organization. Unfortunately, an employee can't start reading the DR Plan when a disaster strikes. Instead, training will help motivate the employee to familiarize themselves with the primary use of equipment in the event of a disaster. The training does not need to be extensive. It should, however, provide a foundation to build on, preparing the employee to comprehend detailed DR processes and procedures in the DR Plan and take on a more demanding recovery role.

15.2 Awareness and Training Approach

For a training program to be effective, it must address major points to ensure the following:

- Key personnel, who are involved in DR, understand the policies and procedures laid out in the plan
- Employees know what procedure to follow when a disaster occurs

- Employees learn how to use disaster management equipment in DR
- Personnel understands their roles and responsibilities in DR
- Full support from Executive Management

The main objective is to create awareness of the DR processes and procedures so that all staff are updated and regularly trained on all recovery procedures.

15.3 Awareness and Training Program Development Process

To develop a practical awareness session or training program, you must adopt a structural approach comprising the following main phases.

15.3.1 Analysis

Analyze the requirements of the awareness session and training program for different audiences, such as management, middle managers, and general staff. Identify the most effective means of communicating with the target audiences.

15.3.2 Sourcing

Sourcing will encompass all required resources to carry out the development of awareness and training programs. Some of these resources include:

- Instructors, both in-house or external, who are suitable to conduct the awareness or training programs
- Materials such as books, video films, posters, etc. Consider whether you can get them off the shelf or if there is a need to engage people to develop them, or whether you can do it in-house
- The appropriate model to adopt for the awareness or training programs. They can take the forms of seminars, lunchtime talks, classrooms, exercises, computer-based e-learning

15.3.3 Development

Develop the various components of the awareness session or training program, such as the session plan, presentation slides, study cases, video films, exercises, test questions, etc.

15.3.4 Delivery

Deliver the awareness sessions and training programs according to the scope, session plan and schedule. Always follow up with an assessment of the session or program effectiveness through feedback forms, discussions or review meetings.

15.3.5 Evaluation

Evaluate the effectiveness of the awareness sessions or training programs through feedback forms and discussions with participants. Then review, refine or even redevelop the program to enhance its effectiveness and results.



15.4 Considerations for Awareness and Training Programs

When designing awareness and training programs, always consider the type of information or knowledge required by the employees, contractors, visitors, managers and individuals who have a role in the DR Plan. In general, some of the topics to look into should at least address the following:

- Threats, hazards, and protective actions.
- Notification, warning and communications procedures.
- Emergency response procedures.
- Evacuation, shelter and accountability procedures.
- Location and use of standard emergency equipment.
- Emergency shutdown procedures.

15.5 Awareness Programs

Awareness of DR plans or activities will increase the efficiency and effectiveness of staff response to disaster situations. For example, if the staff members react to fire alarms by going to the correct exit and assembly area, it will minimize confusion and injuries. Thus, an awareness program is a key factor in enhancing a DR Plan's effectiveness, reducing confusion, reducing recovery time and ensuring that an orderly DR process can be done. This section will share some of the commonly practised awareness programs.

15.5.1 Annual Training Plan

Make the business unit heads accountable for ensuring that staff under their charge are aware of the DR responsibilities, processes and procedures directly under the business unit's charge. They must also ensure that the staff knows what to do to maintain the DR Plan, such as keeping the inventories of vital records, equipment, tools, applications, etc., up-to-date. At the same time, there is also a need to establish a training policy. Therefore, all business unit heads include each staff for at least one training program, regardless of the annual training map's seminars, workshops, talks or discussion sessions.

Reinforce the awareness of the organisation's DR process personnel by making business unit heads accountable for the budget needed to carry out all these DR Plan maintenance work and the DR training courses for the staff.

15.5.2 New Employee Orientation Program

Make it compulsory for all new employees to attend a briefing session on the organization's DR Plan and the expectation of each employee during a disaster situation. Make them sign off after attending the session to reinforce that the organization is serious about the DR program. The HR can also highlight that DR training is part of the annual training plan of the organization.

15.5.3 Posters and Notices

Another way of raising awareness of the DR process in the organization is to put up posters and notices of available DR courses, dates of DR exercises, names of participants of DR exercises, and recognition from Executive Management on the successful execution of DR exercises onto organization notice-boards. Through these publicity channels, staff awareness of DR activities will be increased, and staff will know their effort in DR Planning and maintenance is well appreciated by the management.

However, the shortcoming of this method is you must be able to renew the posters and notices promptly and not leave them there. Otherwise, the adverse effects of an organization's ignorance of DR activities are also easily shown.

15.6 Training Programs

DR training focuses more on skill sets and know-how in performing the DR activities, while awareness programs focus on general knowledge. Some examples of DR training are the technical skills for recovering a Windows NT server and recovering data from backup tapes using backup software such as ARCserve.

In general, DR training can be divided into five major phases: pre-planning, planning, development, testing, and maintenance. For each of these phases, the scope and requirements for the training needs differ to address the needs of different personnel and skill-sets.

15.7 Pre-planning Phase

During the pre-planning phase, the scope and objectives are to equip the key personnel with enough understanding of DR Planning, the methodology for carrying out a proper DR Plan, the needs of having a DR Plan and how to estimate budget requirements for carrying out a DR Plan development and maintenance. In summary, this training phase is to equip the critical DR personnel with the knowledge to justify to the management the need to have a DR Plan for the organization so that sufficient budget, resources, and commitment are given to develop a proper DR plan.

15.8 Project Management Phase

In this project management phase, the training should focus on developing skill-sets to identify the most suitable DR Plan development methodology for the organization. The skills of carrying out risk analysis, assessment and management, and the technical know-

how of carrying out a Business Impact Analysis to ensure that the control of committing their support and endorse the kicking-off of the DR Plan development for the organization.

15.9 Plan Development Phase

The training should focus on specific procedural aspects of developing and implementing the DR Plan in this phase. The training focus will be on the areas of:

- Project management, which is essential for successful DR Plan development
- DR Plan development methodology selected for the organization during the planning phase
- The review process of documentation standards
- DR Plan development software, if chosen for developing the DR Plan
- Definition of specific roles and responsibilities in the execution of the plan
- Identification of interdependencies of individual units' plans to the overall DR Plan
- A thorough understanding of the team checklists of procedures, including notification procedures

15.10 Testing and Exercise Phase

In this training phase, the organization should concentrate on building up staff skill sets to verify and validate the strategies and procedures detailed in DR Plan. At the same time, exercising the DR Plan will also provide unique and valuable training for the DR team members.

The scope of the training should concentrate on getting the staff to:

- Understand the various types of testing methodology
- Define test schedules
- Establish objectives of the test, test criteria, and test scenarios
- Recap any specific technical skill-sets for recovering the IT systems or applications
- Capture test results
- Document results and any lessons learned

Cloud, In addition, develop the skill-sets of carrying out post-test review meetings to capture all the shortcomings, errors, omissions or gaps of the DR Plan against the actual operational environments.

15.11 Program Management Phase

In the program management phase, the training should focus on plan distribution and collection, establishing management control processes for modifying and updating the DR Plan, and establishing the frequency of DR Plan review and updating. At this point, the training is somewhat procedural and sequential. The training sessions must focus on standard documentation formatting, standard procedures for version control, distribution control, and review and approval of updates to planning.

15.12 Conclusion

Training and awareness is an ongoing process and not a one-off event. The DR Plan changes with staff turnover, business environment changes, and hardware, software and application systems upgrades. Thus, continually educating the staff involved in DR with correct and updated skill-sets is critical to the readiness of the organization to respond to disasters. The most vital point is refreshing, refreshing and refreshing the memory of the staff to ensure a complete understanding of all processes and procedures of the DR Plan so that it can work. Without the people with the right skill sets to operate it, a good plan is a useless stack of papers. Training and awareness make a DR Plan work.

16 References

The author acknowledges the following references:

- BCM Institute. (2008). BCMpedia. A Wiki Glossary for Business Continuity Management (BCM), Crisis Communication (CC), Crisis Management (CM), Disaster Recovery (DR) and ISO22301 Audit. *BCMpedia*. Retrieved from http://www.bcmpedia.org/wiki/Business_Continuity_Life_Cycle
- Conner, L., & Dubois, L. (2013). Key Criteria in Selecting a Cloud Backup Provider Built to Last. *IDC WhitePaper*, (May). Retrieved from file:///C:/Users/Dr Goh Moh Heng/Documents/Upload Cloud/IDC_Cloud_Provider_Key_Criteria_US.pdf
- Courtney, Neal (1999), Developing Business Continuity Strategies for Business or Work Area, *The Definitive Handbook of Business Continuity Management*, pg 151 to 161.
- Fulmer, Kenneth L. (2000): *Business Continuity Planning, 2000 Edition: A Step-By-Step Guide with Planning Forms*.
- Gibilisco, S. (2014). Definition: Disaster Recovery as a Service (DRaaS). *Tech Target*, (Feb).
- Goh, M. H. (2006). *Testing and Exercising Your Business Continuity Plan. Business Continuity Management Series* (2nd ed.). Singapore: GMH Pte Ltd.
- Goh, M. H. (2008a). *Analyzing and Reviewing the Risks for Business Continuity Planning. Business continuity management series* (1st ed.). Singapore: GMH Pte Ltd.
- Goh, M. H. (2008b). *Conducting Your Impact Analysis for Business Continuity Planning. Business Continuity Management Series* (2nd ed.). Singapore: GMH Pte Ltd.
- Goh, M. H. (2008c). *Managing Your Business Continuity Planning Project. Business Continuity Management Series* (2nd ed.). Singapore: GMH Pte Ltd. Retrieved from http://www.bcmpedia.org/wiki/Author_of_BCM_Books
- Goh, M. H. (2009). *Developing Recovery Strategy for Your Business Continuity Plan. Business Continuity Management Series* (1st ed.). Singapore: GMH Pte Ltd. Retrieved from http://www.bcmpedia.org/wiki/Author_of_BCM_Books
- Goh, M. H. (2010a). *Implementing Your Business Continuity Plan. Business Continuity Management Series* (2nd ed.). Singapore: GMH Pte Ltd.
- Goh, M. H. (2010b). *Managing and Sustaining Your Business Continuity Management Program. Business Continuity Management Series* (1st ed.). Singapore: GMH Pte Ltd. Retrieved from http://www.bcmpedia.org/wiki/Author_of_BCM_Books
- Goh, M. H. (2016a). *A Manager's Guide to Implement Your Crisis Communication Plan. Business Continuity Management Specialist Series* (1st ed.). Singapore: GMH Pte Ltd.
- Goh, M. H. (2016c). *Dictionary of Business Continuity Management. Business Continuity Management Dictionary Series* (5th ed.). Singapore: BCM Institute.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Hiles, Andrew & Barnes, Peter (ed) (2001): Definitive Handbook Business Continuity Management, 410 pages.
- ISACA. (2012). Business Continuity Management : Emerging Trends. *ISACA EmergingTechnology White Paper*, (Dec).
- ISO 22301. (2012). ISO22301:2012 Societal Security – Business Continuity Management Systems – Requirements. Societal Security – Business Continuity Management Systems – Requirements (1st ed.). Switzerland: International Organization for Standardization.
- James C. Barnes (2001): A Guide to Business Continuity Planning, 174 pages.
- Ken Doughty (ed) (2000): Business Continuity Planning: Protecting Your Organization's Life, 400 pages.
- Mircea, M., & Andreescu, A. (2011). Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. *Communications of the IBIMA*. <http://doi.org/10.5171/2011.875547>
- Online Tech. (2015). Benefits of Disaster Recovery in Cloud Computing. *Online Tech*. Retrieved from <http://www.onlinetech.com/resources/references/benefits-of-disaster-recovery-in-cloud-computing>
- Peter Gregory (2007): IT Disaster Recovery Planning For Dummies, 360 pages.
- Rothstein, P Rothstein (2001) Choosing A Hot-site Vendor.



Appendices

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Technical DR Considerations

- A End-User Computing
- B Servers
- C Local Area Networks
- D Wide Area Networks

Appendices

- E Sample Table of Content of DR Plan
- F A Sample Format of a DR Plan
- G A DR Planning Project – Major Activities/Milestones
- H DR Site - Selection & Evaluation Checklist
- I A Sample Questionnaire for Conducting Business Impact Analysis Interviews
- J A Sample Table of Content of Request For Proposal
- K A Sample of the DR Test Checklist
- L A Sample of DR Test Design Template
- M Frequently Asked Questions

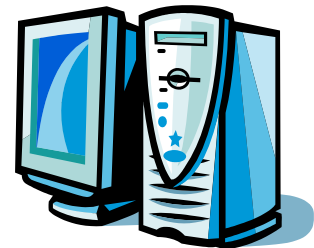
17 Appendix A - Technical DR Considerations - End User Computing

17.1 Overview

End-User Computing (EUC) Resources can be classified into two major categories: fixed-based and mobile.

17.1.1 Fixed Based Computing

These resources include desktop computers, workstations, printers, scanners and items that are not easy to be moved around with their users.



17.1.2 Mobile Computing

These resources refer to laptop computers, notebooks, handheld devices and items that users can easily carry around.

Most desktops are networked to cater for communications with other networked devices, applications and the Internet. Portable systems, such as laptops (also called notebook computers) or handheld computers, are PCs that can be carried for convenience and travel purposes. Portable systems can connect to other networked devices, applications and the Internet through various mechanisms, such as dial-up lines.

Desktop and portable computers are the most common platform in any organization's IT infrastructure as they are required for routine automated processes. Therefore, the virtue and mass population of these desktop devices in the organization have become essential elements in a DR Plan.

17.2 Technical DR Considerations

The core DR concerns for each desktop and portable system are data availability, confidentiality, and integrity. Some of the key considerations when planning for DR are:

17.2.1 Encourage Individuals to Backup Data Regularly

Encourage users to regularly back up their critical data stored on a desktop or portable system. This can be done through education and awareness programs. In addition, the IT

business unit may want to consider implementing automated PC backup through network backup technologies for primary users.

17.2.2 Store Backups Offsite

Backup media should be stored offsite in a secure, environmentally controlled facility. If users back up data on a stand-alone system rather than saving data to the network, a means should be provided for storing the media at an alternate site. A copy of the DR Plan, software licenses, vendor SLAs and contracts, and other relevant documents should be stored with the backup media.

17.2.3 Provide Guidance on Saving Data on Personal Computers

Users are strongly advised to save very critical data in a particular folder on the business initially shared folders on the file and print server. Doing so will increase the data protection capability as server backups are done daily and help the technician speed up the recovery of the individual desktop.

17.2.4 Standardized Hardware, Software, and Peripherals

System recovery is faster if hardware, software, and peripherals are standardized. If standard configurations are not possible throughout the organization, then configurations should be standardized by business unit, machine type, or model.

Additionally, critical hardware components to be recovered immediately in a disaster should be compatible with off-the-shelf computer components. This compatibility will avoid delays when ordering custom-built equipment from a vendor.

17.2.5 Document System Configurations and Vendor Information

Well-documented system configurations aid the recovery process. Similarly, vendor names and emergency contact information should be listed in the DR Plan to purchase replacement equipment quickly.

17.2.6 Alignment With Organisation's Network Security and System Access Security Policy

Align desktop recovery requirements to the network and security control. For example, virus protection can help protect against malicious code or attacks that could compromise the computer system's availability. Data confidentiality and sensitivity requirements should be considered in choosing the appropriate technical DR solution to ensure that the technical DR solution does not compromise or disclose sensitive, proprietary or classified data.

17.3 Considerations for Choosing DR Solutions

Wide ranges of technical DR solutions are available for desktop computers. Some of the backup solutions and backup media are listed in the following sections.

Backup is necessary to ensure data availability on desktops and portable computers. Thus, we must consider carefully all the following factors that will affect our selection of an appropriate backup solution.

17.3.1 Equipment Interoperability

In order to facilitate recovery, the backup device must be compatible with the platform operating system and applications and should be easy to install onto different models or types of PCs.

17.3.2 Storage Volume / Data Size

The amount of data to be backed up should determine the appropriate backup solution to ensure adequate storage.

17.3.3 Media Life

Each type of media has a different use and storage lifespan beyond which the media cannot rely for effective data recovery.

17.3.4 Backup Software

When choosing the appropriate backup solution, the software or method used to backup data should be considered. The backup application can sometimes be as simple as a file copy using the operating system file manager. A third-party application may be needed to automate and schedule the file backup in cases involving larger data transfers.

17.4 Data Backup Media

The key to successful backup is the media. The media with the actual capacity, material, and size will determine the backup and recovery operations speed. The details of each type of these backup media are discussed as follows:

17.4.1 Portable Drives

Portable drives can be easily purchased, and they are the cheapest backup solution. However, these drives pose a security risk when misplaced.

17.4.2 Tape Drives

Tape drives are not common in desktop computers but are an option for a high-capacity backup solution. Tape drives can be automated and require a third-party backup application or backup capabilities in the operating system. In addition, tape media are relatively low cost.

17.4.3 Removable Cartridges

Removable cartridges are not standard in desktop computers and are often offered as a portable or external device backup solution. Removable cartridges are more expensive than floppy diskettes and are comparable in cost to tape media, depending on the media model and make. However, removable cartridges are fast, and their portability allows for flexibility.

The portable devices come with special drivers and applications to facilitate data backups.

17.4.4 DVD & CD-ROM

DVD & CD-ROM, read-only memory (ROM) drives come standard in most desktop computers. DVDs are low-cost storage media and have a higher capacity than floppy diskettes. The operating system's file manager is sufficient; however, a writable (DVD-R) or rewritable DVD (DVD-RW) drive and the appropriate software will be required to write to a DVD. This technology is now deemed to be obsolete.

17.4.5 Network Storage

Data stored on networked PCs can be backed up to a networked disk or a network storage device.

In a Networked Disk environment, users' data are backed up onto a standard server's hard disk partition. Thus, the amount of data that can be backed up from a PC is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up by the network or server backup program.

A network backup system will be configured to back up the local drives on networked PCs in a Networked Storage Device environment. The backup can be started from either the networked backup system or the actual PC.

17.4.6 Disk Imaging

Disk Imaging is a DR solution that duplicates the particular application and configuration, but not the data, of the desktop where the disk image is performed. The disk image produced is usually huge, but it is a quick desktop reconstruction tool to recover the original setup. The limitation of disk imaging is that it can only be done on the exact model and identical hardware configuration desktops.

17.4.7 Power Supplies

The system and its data can become corrupted due to a power failure. A PC can be configured with dual power supplies to prevent corruption. The two power supplies should be simultaneously used. If the main power supply becomes overheated or unusable, the second unit will become the primary power source, resulting in no system disruption.

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

The second power supply will protect against hardware failure, not a power failure. However, a UPS can protect the system if power is lost. A UPS usually provides 30 to 60 minutes of temporary backup power which may be enough to permit a graceful shutdown. A cost-benefit analysis should compare the dual power supply and UPS combination. Although dual power supplies and UPS are cost-effective for a server, they may not be appropriate or economical for a PC.

18 Appendix B - Technical DR Considerations – Servers

18.1 Overview

A server is a central computer in a network to which other computers or terminals are connected. It has shared programs, files, and databases stored on the server

A server can be a desktop computer, a mid-range machine such as an HP, SUN, IBM or Dell server, a large mainframe computer, or any computing hardware capable of processing a high volume of transactions. What makes a server different from a normal computer is that a server is designed to:

- Share multiple IT resources such as sharing of printers and disks storage
- Perform sophisticated and specific functions in the areas of application usage's authentication, user access control and password management
- Host central databases and applications such as email services

18.2 DR Consideration

Servers are usually used to support the operation of critical business processes. Thus, any interruptions to the server or its components will disrupt the server's capability to support the business processes. Depending on the extent of the disruption, some incidents may incur a few business losses, and others may severely impact the customers and cause the organization to close its operation.

Thus, to safeguard the organization's business from being destroyed by potential disasters, the Organization DR Coordinator should consider the following practices carefully when designing the server recovery strategy.

18.2.1 Offsite Storage for Backup Media

The offsite storage facility that is chosen to store the backup media containing critical applications, data and system software should have the following characteristics:

- Equipped with adequate security and environmental controls, and management mechanisms
- Located far enough away from the original site to reduce the likelihood that both sites would be affected by the same incident
- Able to access facility, e.g. 24 hours by seven days

18.2.2 Standardized Hardware and Software

The hardware, software, and peripherals must be standardized throughout the organization to conduct a faster system recovery of servers. If standard configurations are not possible throughout the organization, then configurations should be standardized by business units, machine type, or model.

In addition, the sourcing and procuring of new critical hardware components that are to be recovered immediately in a disaster should be compatible with off-the-shelf computer components. This compatibility will avoid delays when ordering custom-built equipment from a vendor.

18.2.3 Special Agreement with Manufacturer

Suppose the organization has specific critical hardware or systems specially tailored to its design and installation and proprietary to its manufacturer. In that case, there is a need to consider establishing a special agreement with its manufacturer to provide redundancy and backup to ensure continued availability.

18.2.4 System Configurations and Vendor Information

Well-documented system configurations aid the recovery process. Similarly, vendor names and emergency contact information should be listed in the DR Plan to purchase replacement equipment quickly.

18.2.5 Alignment with Security Policy

Aligning server recovery requirements to the network and security controls, such as virus protection, can help protect against malicious code or attacks that could compromise the computer system's availability. Data confidentiality and sensitivity requirements should be considered when choosing the appropriate technical DR solution to ensure that the technical DR solution does not compromise or disclose sensitive, proprietary or classified data.

18.3 DR Solutions

There are many server recovery technologies available in the market. However, the selection criteria should be measured against the risks of the business and the investment and maintenance cost of that particular recovery technology. The Organization DR Coordinator may use the quantifiable risks identified in the BIA process as an excellent supporting justification for the investment required for adopting the appropriate recovery solution.

In designing the server's DR Plan, the emphasis should be on the recovery reliability, efficiency, practicality and feasibility of maintenance. At the same time, the recovery solution should also cover the end-to-end availability to include all networks, servers and applications services.

Some of the leading recovery technologies available for server recovery are listed in the following sections, such as Resiliency and Virtualization.

18.4 System Backup Methodology

Some principal system backup methodologies include Full, Incremental and Differential backup practices. The details of these backup technologies are explained in **Chapter 7** of this book. To supplement the explanation provided in Chapter 7, you might also want to consider the following pointers when establishing the server's backup and recovery plan:

- Where should the backup media be stored?
- What data should be backed up?
- How frequent and at what time should the backups be conducted?
- How quickly can the backup media be retrieved in an emergency? (Including after office hours and weekends)
- Who should authorize the retrieval of the media?
- Where will the backup media be delivered?
- Who will be responsible for restoring the data from the media?
- What is the tape labelling scheme?
- How long will the backup media be retained?
- When are the media stored onsite, and what environmental controls are provided to preserve the media?
- What types of tape readers are used at the alternate site?

18.5 Quality of Storage Media

To perform successful recovery of any server is not only about the backup and recovery process alone but also about the recoverability and quality of the backup media used. And some of the good practices to maintain the quality of the backup media are listed as follows:

- Keep tapes and cartridges dry and clean
- Maintain tape drives regularly
- Test restoration regularly
- Do not exceed the useful lifespan of the tapes
- Keep tapes in a suitable environment with the correct humidity and temperature.

18.6 Offsite Media Storage

Backup media should be stored offsite in a secure and controlled environment. When selecting the offsite location, the following pointers should be taken into consideration:

- Physical separation from the location of the primary server
- Ease of retrieving the backup media, especially during weekends, after office hours and public holidays
- The turnaround time to retrieve backup media should be reasonably short to meet your RTO
- Physically secured environment and appropriate air conditioning and humidity control suitable for storing tapes and cartridges
- Safety of the surrounding environment, e.g. not exposed to fire, flood and proximity to any high-risk facility (e.g. petrol kiosks, government offices)
- For the backup location, which external vendors provide, it is vital that the confidentiality, security and accessibility are clearly defined in the service contract

18.7 Resiliency Technologies

Redundancy is the key factor for reaching a server's resilience. Thus, selecting a suitable and economic redundancy technology is necessary to ensure the availability of data and business operations.

Some of the redundancy technologies available in the market are listed in the following subsections.

18.7.1 RAID

RAID, an acronym for Redundant Array of Independent Disks, provides disk redundancy and fault tolerance for data storage. RAID subsystem consists of multiple "paths" connected to the servers. If a 'path' fails, the servers can continue accessing the data on other surviving 'paths'. In addition, with a RAID system, the disk can be hot-swappable without shutting down the system for replacement.

18.7.2 Clustering

Several servers can be interconnected as a 'cluster' such that if one of the servers is not working, its applications can be automatically switched to other servers in the cluster.

- **Load Balancing**

Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server in the network. Load balancing systems monitor each server to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable DR measure depending on system availability requirements.

18.7.3 Remote Journaling and Electronic Tape Vaulting

Electronic vaulting and remote journaling use similar technologies that enable data backup to remote tape drives via communication links. Both solutions provide shorter recovery times and reduced data loss.

■ Electronic Vaulting

With electronic vaulting, the system is connected to an electronic vaulting provider to automatically allow backups to be created at the offsite tape drives.

The electronic vault could use optical disks, magnetic disks, mass storage devices, or an automated tape library as storage devices. This technology transmits data to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling.

■ Remote Journaling

With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals might be used to recover transactions, applications, or database changes after the last server backup. Remote journaling can be carried out during batches or continuously communicated using buffering software. Remote journaling and electronic vaulting require a dedicated offsite location to receive the transmissions. The site can be the system's hot site, offsite storage site, or another suitable location. Depending on the volume and frequency of the data transmissions, remote journaling or electronic vaulting could be implemented over limited bandwidth.

18.7.4 Data Replication

Data replication technology uses the concept of replicating critical data on two or more disks, on either one physical hardware or over a group of logical hardware. Thus, when one of the mirrored disks fails, the surviving disks take over transparently. There are two main data replication techniques available, and they are:

□ Synchronous

This method uses a disk-to-disk copy and maintains a replica of the database or file system by applying changes to the replicating server. In contrast, transformations are applied to the protected server.

The synchronous mode can potentially degrade performance on the protected server, and it demands high bandwidth. Thus, the synchronous mode should be implemented only over shorter physical distances, such as campus-wide networks, whereby the cost of bandwidth is not a constraint and is suitable for critical applications that can accept little or no data loss.

□ Asynchronous

This method maintains a replica of the database or file system by continuously capturing changes to a log and replicating the changes in the log to the remote disk. This method has little impact on performance, and it utilizes less bandwidth; hence applicable for replication over longer distances with inherits network latency.

18.8 Storage Virtualization

Storage virtualization combines multiple physical storage devices into a logical, virtual storage pool that can be centrally managed and is presented to network applications, operating systems, and users as a single storage device. The benefits of storage virtualization are that storage devices can be added without requiring network downtime, storage volumes from a downed server or a storage device can be reassigned, and the assigned storage for a server can be easily created, deleted, or expanded on to meet the server's requirements. Some of the storage architectures that are available in the market to support storage virtualization include:

❑ Network Attached Storage (NAS)

NAS is a concept of shared storage on a network by separating the storage resources from network and application servers. Generally, NAS environments are file-oriented and offer a common storage area for multiple servers on a dedicated, high-performance file server. And NAS uses file-oriented protocols for all applications to send data to or receive data from a NAS device.

❑ Storage Area Network (SAN)

SAN is a defined architecture consisting of a server and storage network. As opposed to a NAS, a SAN provides data access in blocks and is built to handle storage and backup traffic instead of file-orientated traffic. A SAN can be local or remote (within a limited distance) and usually communicates with the server over a fibre channel.

The SAN solution moves data storage of the LAN, thus enabling backup data to be streamed to high-speed tape drives, which does not affect network resources as distributed and centralized backup architecture does.

19 Appendix C - Technical DR Considerations – Local Area Networks

19.1 Overview

A **Local Area Network (LAN)** is a combination of hardware and software technology that allows computers to share various resources, such as electronic data, applications, printers and storage devices, all confined within a building or a small group of buildings. In addition, LANs also allow messages to be sent between attached computers, thereby enabling users to work together electronically in a process often referred to as collaborative computing.

Several LAN topologies are available in the market, and major ones are listed in the following table:

LAN Topologies	Description
Mesh	Networked components are connected with many redundant interconnections between network nodes.
Star	All nodes are connected to a central hub.
Bus	All nodes are connected to a central cable called a bus or backbone.
Ring	All nodes are connected in the shape of a closed loop so that each node is directly related to two other nodes, one on either side of it.
Tree	A tree is a hybrid topology where a linear bus backbone connects star-configured networks.

The LAN architectures vary from peer-to-peer. Each node is equivalent to any other node in terms of responsibilities, and client/server setup, whereby a client node depends on the server node for resources. Thus, as there are differences in topologies, architectures and protocol variations in different organizations, DR solutions will vary accordingly.

19.2 DR Considerations

When developing the LAN recovery strategy, the Organization DR Coordinator should consider some of the following key points before deciding on a solution for the organization:

19.2.1 Network Diagrams and Configuration Information

Up-to-date network diagrams and detailed configuration information for each networking device, such as routers, switches, bridges and hubs, must be well kept as it will greatly help the recovery team restore the LANs swiftly and quickly.

There following are two different types of network diagrams that you will need to take note of and maintain:

- Logical network diagram, which presents the LAN and its nodes. Network discovery software can provide an accurate picture of the LAN
- Physical network diagram, which displays the physical layout of the facility that houses the LAN and cable jack numbers

19.2.2 Vendors Contacts

Contact details for core network equipment vendors must be kept in the DR Plan so that during the disaster, they can be contacted immediately to replace all network equipment and firmware.

19.2.3 Alignment with Organisation's Network Security and System Access Security Policy

LAN DR solutions should be aligned with network security policies to protect against threats that could disrupt the network. Leverage the impacts and priorities of critical business applications derived from the BIA exercise to determine the LAN recovery priorities.

19.3 Considerations for Choosing DR Solutions

When developing the LAN DR Plan, the Organization DR Coordinator should:

19.3.1 Identify Single Points of Failure

The Organization DR Coordinator should identify all potential single points of failure that will affect the critical systems or processes outlined in the BIA. This analysis could include threats to the cabling system, such as cable cuts and electromagnetic and radio frequency interference. Even damage caused by fire, water, and other hazards should be considered. As a solution, redundant cables may be installed where appropriate. For example, installing duplicate cables to desktops might not be cost-effective. However, it may be worthwhile installing a 100-megabit cable between floors.

19.3.2 Identify Network Connection Points

Consider all the network connecting devices, such as hubs, switches, routers, and bridges. The BIA should characterize each device's roles in the network, and a DR solution should be developed for each device based on its BIA criticality. As an example of a DR strategy for network connecting devices, redundant intelligent network routers may be installed in a network, enabling a router to assume the full traffic workload if the other router were to fail.

19.3.3 Remote Accessibility

Remote access is a service that allows users working offsite to communicate with servers and devices in the office. Remote access can be conducted through various methods, including dial-up access and virtual private network (VPN). In an emergency or severe system disruption, remote access may serve as a critical DR capability by providing access to organization-wide data for recovery teams or users from another location. Data bandwidth requirements should be identified and used to scale the remote access solution if remote access is established as a DR strategy.

19.3.4 Wireless Connectivity

Wireless local area networks also can serve as an effective DR solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs, so they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. Security controls, such as data encryption, should be implemented when implementing a wireless network if the communications traffic contains sensitive information.

19.3.5 Network Monitoring Software

Network monitoring software is an excellent tool to pre-empt a LAN disruption to reduce its impact. The software issues an alert if a node or device begins to fail or is not responding. The administrator often receives a warning from users, and other nodes notice problems. Many types of monitoring software may be configured to automatically send an electronic page to a designated individual when a system parameter falls out of its specification range.

20 Appendix D - Technical DR Considerations - Wide Area Networks

20.1 Overview

Wide Area Network (WAN) is a data network that interconnects two or more LANs across different geographical locations within the boundary of a country or other countries. In addition, a WAN can also be connected to another WAN for information communication needs.

The major telecommunication technologies that are used to interconnect the WAN between LANs or WANs can be classified as follows:

20.2 Dial-up

Dial-up connections leverage the existing analogue telephone network infrastructure through modems. The dial-up connection can achieve a maximum of 56kbps of data communication theoretically. As such, dial-up is only suitable for minimal data transfer over a non-permanent connection.

20.3 ISDN

Integrated services digital network (ISDN) is an international communications standard for sending voice, video, and data over digital or standard telephone wires. The data transfer rates for an ISDN connection can be in the form of channels of 64kps. However, it typically comes in two channels or 30 channels of 64kbps.

20.4 DSL

Digital Subscriber Line (DSL) is a technology that dramatically increases the digital capacity of ordinary telephone lines in the home or office. And unlike ISDN, which is also digital but travels through the switched telephone network, DSL provides an "always-on" operation.

20.4.1 Leased Lines

A leased line is a dedicated phone connection supporting fixed data rates between two LANs located in two different geographical locations. Some of the typical leased lines are:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- The t-1 line consists of 24 64 kbps channels, and each can be configured to carry voice or data signals. Fractional T-1 access also can be provided when multiples of 64 kbps lines are required
- E-1 line that supports 2Mbps of data transfers speed
- A T-3 line consists of 672 individual channels, each supporting 64 Kbps. T-3 is also referred to as DS3

20.4.2 ATM

ATM is a network technology that transfers data at high speeds using fixed-sized packets. ATM implementation supports data transfer rates from 25 to 622 Mbps and provides guaranteed throughput.

20.4.3 Frame Relay

Frame relay is a packet-switching protocol for connecting devices on a WAN. In frame relay, data is routed over virtual circuits. Frame relay networks support data transfer rates at T-1 and T-3 speeds.

20.4.4 SONET

Synchronous Optical Network (SONET) is the standard for synchronous data transmission on optical media. SONET supports gigabit transmission rates.

20.4.5 Wireless

A wireless LAN bridge can connect multiple LANs to form a WAN. Wireless supports 20 to 30 miles with a direct line of sight.

20.4.6 VPN

A VPN is an encrypted channel between nodes on the Internet over public networks.

20.5 Technical DR Considerations

The core DR consideration for recovering the WAN setup during any disruptions is the speed of restoring the WAN services in the shortest possible time to support the quick recovery of the business applications to satisfy the organizational RTO and RPO requirements.

To support this core consideration, we must equip the recovery personnel with the correct information, technical skill sets, complete recovery procedures, and tools to enhance their ability to speed up recovery. Some of the good DR practices you may want to consider for improving the comprehensiveness of the WAN recovery process are listed in the following subsections.

20.5.1 Technical Documentation

Precise and up-to-date WAN architecture diagram with the following details:

- Brand, model, serial number and firmware version of all network-connected devices that are needed to set up the WAN
- IP addresses that are assigned to every of the network devices
- Configurations of each of the network devices and where the backup copies of the configuration data are stored
- Type of communication links used, vendors who provide the links and the geographical locations where these links are connected to
- Contact information for all the vendors
- Contract documents or agreements with all the vendors
- SLA expectations for carrying equipment replacement, a swing of links to backup sites, switching over to backup links, redirecting telecommunication services to alternate service providers, etc.
- Alignment with Organisation's Network Security and System Access Security Policy

Coordinating the WAN DR solutions with the organization's network security and system access policies will enable you to protect your WANs against potential threats, such as virus infections and DDOS, that will affect your network availability.

- Alignment of Criticality of WAN Services with Data and Applications

WAN DR strategies are influenced by the type of data routed on the network. For example, a WAN that hosts a mission-critical distributed system will require a more robust recovery strategy than a WAN that connects multiple LANs for simple resource-sharing purposes.

20.6 DR Solutions

The basis of WAN DR solutions includes all the measures discussed for PCs, servers, websites and LANs that we have discussed in the previous Appendices. In addition, this chapter will add additional recovery solutions that address the area of communications links that connect the separate LANs.

20.6.1 Redundancy of Communications Links

Redundant communications links usually are necessary when the network processes critical data. The redundant links could be the same type, such as two T-1 connections, or the backup link could provide reduced bandwidth to accommodate only essential transmissions of a DR situation.

For example, an ISDN line could be used as a DR communications link for a primary T-1 connection. If redundant links are used, the Organization DR Coordinator should ensure

that the links have physical separation and do not follow the same path; otherwise, a single incident, such as a cable cut, could disrupt both links and render this strategy useless.

20.6.2 Redundancy of Network Connecting Devices

The duplicating network connecting devices, such as routers, switches, and firewalls, can improve the network availability of the LAN interfacing points by removing the risk of single points of failure at the LAN interfaces. At the same time, this solution will also improve the WAN's communication speed by using load-balancing techniques over the primary and backup network devices.

20.6.3 Redundancy of Network Service Providers

If 100 per cent data availability is required, redundant communications links can be provided through multiple Network Service Providers (NSPs). In addition, to provide further redundancy, independent Internet connections may be established from two geographically separated LANs. Internet traffic could be routed through the remaining connection when one connection fails.

If this solution is chosen, the Organization DR Coordinator should:

- Ensure the NSPs do not share common facilities at any point, including building entries or demarcations
- Consult with the selected NSP or Internet Service Provider (ISP) to assess the robustness and reliability within their core networks (e.g., the redundant network connecting devices and power protection)

However, this strategy highlights the balance that must be maintained for security and availability. Multiple Internet connections increase a network's vulnerability to hackers.

20.6.4 Tighten Service Level Agreements with Network Service Providers

SLAs can facilitate prompt recovery following software or hardware problems associated with the network. An SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs if the vendor's network is unavailable. If the NSP or ISP is contracted to provide network-connecting devices, such as routers, the availability of these devices should be included in the SLA.

21 Appendix E: A Sample Table of Contents of the DR Plan

21.1 Explanation

This is a sample of the Table of Contents for a typical DR Plan. This will assist the Organization DR Coordinator in conducting an initial assessment of the efforts, timeline, and budget required to develop a DR Plan.

The subject shown below served as a guideline for developing a DR Plan. The Organization DR Coordinator must modify the Table of Contents to meet their specific organizational requirements.

Sample DR Plan Table of Contents

1.0	Overview	1
1.1	Objectives	2
1.2	DR Plan Scope	3
1.3	Policies Statement	3
1.4	Plan Approval	4
1.4	Board and Executive Management Responsibilities	5
1.5	Assumptions	6
1.6	Definition of Disaster	7
2.0	Business Impact Analysis	8
2.1	Scope	9
2.2	Objectives	10
2.3	Critical Timeframe	11
2.4	Application System Impact Statements	12
	2.4.1. Essential	13
	2.4.2. Delayed	14
	2.4.3. Suspended	15
2.5	Summary	16
3.0	Recovery Strategy	17
3.1	Approach	18
3.2	Cost Benefits Analysis	19

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

3.3	Escalation Plans	20
3.4	Decision Points	21
3.3.1	'GO' PLAN	22
3.3.2	'NO-GO' PLAN	23
4.0	Disaster Recovery Organization	24
4.1	Recovery Organization Chart	25
4.2	Disaster Recovery Team	26
4.3	Recovery Team Responsibilities	27
4.3.1	Recovery Management	28
4.3.1.1	Pre-Disaster	29
4.3.1.2	Recovery Execution	30
4.3.1.3	Post-Disaster/Return Home	31
4.3.2	Recovery Manager Responsibilities	32
4.3.2.1	Pre-Disaster	33
4.3.2.2	Disaster Recovery	34
4.3.2.2	Post-Disaster/Return Home	35
4.3.3	Damage Assessment and Salvage Team Responsibilities	36
4.3.3.1	Pre-Disaster	37
4.3.3.2	Disaster Recovery	38
4.3.3.3	Post-Disaster/Return Home	39
4.3.4	Physical Security	40
4.3.4.1	Pre-Disaster	41
4.3.4.2	Disaster Recovery	42
4.3.4.3	Post-Disaster/Return Home	43
4.3.5	Information/Computer Security	44
4.3.5.1	Pre-Disaster	45
4.3.5.2	Disaster Recovery	46
4.3.5.3	Post-Disaster/Return Home	47
4.3.6	Administration	48
4.3.6.1	Pre-Disaster	49
4.3.6.2	Disaster Recovery	50
4.3.6.3	Post-Disaster/Return Home	51
4.3.7	Hardware Installation	52
4.3.7.1	Pre-Disaster	53
4.3.7.2	Disaster Recovery	54
4.3.7.3	Post-Disaster/Return Home	55
4.3.8	Systems, Applications and Network Software	56

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

4.3.8.1	Pre-Disaster	57
4.3.8.2	Disaster Recovery.....	58
4.3.8.3	Post-Disaster/Return Home	59
4.3.9	Communications	60
4.3.9.1	Pre-Disaster	61
4.3.9.2	Disaster Recovery.....	62
4.3.9.3	Post-Disaster/Return Home	63
4.3.10	Operations	64
4.3.10.1	Pre-Disaster	65
4.3.10.2	Disaster Recovery.....	66
4.3.10.2	Post-Disaster/Return Home	67
5.0	Disaster Recovery Emergency Procedures	68
5.1	General	69
5.2	Recovery Management	70
5.3	Damage Assessment and Salvage	71
5.4	Physical Security	72
5.5	Information/Computer Security	73
5.5	Administration	74
5.6	Hardware Installation	75
5.7	Systems, Applications & Network Software	76
5.8	Communications	77
5.9	Operations	78
6.0	Plan Administration	79
6.1	Organization DR Coordinator Manager	80
6.2	Distribution of the Disaster Recovery Plan	81
6.3	Maintenance of the Business Impact Analysis	82
6.4	Training of the Disaster Recovery Team	83
6.5	Testing of the Disaster Recovery Plan	84
6.6	Evaluation of the Disaster Recovery Plan Tests	85
6.7	Maintenance of the Disaster Recovery Plan	86
7.0	Appendices	87
	Recovery Team Phone/Address List	88
	Vendor Phone/Address List	89
	Off-Site Inventory	90
	Hardware/Software Inventory	91
	People Interviewed	92

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Preventative Measures 93
Sample Application Systems Impact Statement 94

22 Appendix F: A Sample DR Plan

22.1 Explanation

This sample DR Plan serves as a guide to assist the reader in developing an information technology (IT) DR Plan. The Organization DR Coordinator should modify the format and information to meet the organization's policy and standards and comply with regulatory requirements.

DR PLAN (Sample)

22.2 INTRODUCTION

22.3 Overview

Provide a general description of IT functions. For example, indicate the operating environment, physical location, the general location of users, and partnerships with external organizations/systems. In addition, include information regarding other technical considerations important for recovery purposes, such as backup procedures, information security, etc.

22.4 Purpose

This {*IT organization name*} DR Plan establishes procedures to recover all critical IT services to support the business continuity plan as identified in the Business Impact Analysis following a major disruption.

This plan is developed based on the following objectives:

- Maximize the effectiveness of DR operations through established procedures that consist of the following phases:
 - Notification/Damage Assessment Phase
 - Activation Phase
 - Mobilization Phase
 - Recovery Phase
 - Return to Normal Phase
- Maintain consistency, reliability and workability of the plan through a defined test strategy and procedures

- Establish comprehensive awareness and training strategy and procedures to ensure IT staff is familiar with the plan

22.5 Scope

22.5.1 Scope of the Plan

The scope of this plan describes procedures to recover all critical services following a major disaster that inhibits *{IT organization name}* from continuing to provide services.

The plan design is based on the following disaster scenarios:

- Scenario 1: The *{Organization name}*'s IT facility in *{City, State}*, is inaccessible; therefore, *{IT organization name}* is unable to continue processing from this location
- Scenario 2: Any severe incident causing infrastructure supporting IT and equipment failure impact *{IT organization name}* ability to recover and continue operations from its original location

22.5.2 Assumptions

The following assumptions are considered when developing the DR Plan:

- The *{IT organization name}* is inoperable and cannot be recovered from its original location within *{XX}* hours. (This requirement has to be agreed upon within the organization. In addition, the duration specified must match the defined IT recovery capability. For instance, if the IT recovery capability is 24 hours, this requirement should be longer than 24 hours.)
- A valid contract exists that designates that the site in *{City, State}* as the *{Organization name}*'s alternate operating facility
 - *{Organization name}* will use the *{alternate site}* building and information technology resources to recover *{IT organization name}* functionality during an emergency situation that prevents access to the *{original facility}*.
 - The designated computer system at the *{alternate site}* has been configured to begin processing *{system name}* information.
 - The *{alternate site}* will continue *{system name}* recovery and processing throughout disruption until the return to normal operations.
- Current backups of the application software and data are intact and available at the *{offsite storage facility}*
- The equipment and network are available with adequate capacities at the *alternate site* in *{City, State}*
- Service agreements are established and maintained detailing hardware, software, and communications providers to support the emergency system recovery

The *{IT organization name}* DR Plan does not apply to the following situations:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Major single incident impacting both the original location and the alternate backup location
- Total people loss resulting in *{IT organization name}*'s inability to perform its recovery operations
- Operating System bugs, software problems, and viruses that would impact both production and the backup
- Any additional constraints should be added to this

22.6 Responsibility

The following teams have been developed and trained to respond to a DR event affecting the IT system.

The DR Plan establishes several teams to participate in recovering *{system name}* operations. The *{team name}* is responsible for the recovery of the *{system name}* computer environment and all applications. Members of the *{team name}* include personnel responsible for the daily operations and maintenance of *{system name}*. The *{team leader title}* directs the *{team name}*.

Describe each team's responsibilities, leadership, and coordination with other applicable teams during a recovery operation.

The relationships between the team leaders involved in system recovery and their member teams are illustrated in Figure *{YY}* below.

(Insert hierarchical diagram of recovery teams. Show team names and leaders. Do not include actual names of personnel.)

Describe each team separately, highlighting overall recovery goals and specific responsibilities.

Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

Person Responsible	Responsibility
Organization DR Coordinator	Ensure that the plan is up-to-date and in compliance with organization standards and regulatory policies: coordinate plan reviews and testing of the DR Plan. Conduct DR Plan awareness training.
Technical Support Team Manager	Document and maintain all server recovery procedures and setup for all systems.
Data Centre Operations Manager	Maintain all operations procedures required to support backup and recovery operations.
Network Manager	Maintain all network backup and procedures to support network recovery.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Person Responsible	Responsibility
Desktop / Distributed Technology Support Manager	Maintain all desktop and distributed technology infrastructure setup and recovery procedures.
Change Control Manager	Keep track of changes and ensure the DR team reviews changes that could impact the recovery plan.
Information Security Manager	Ensure security information controls are maintained.
Media and Vital Records Control Manager	Ensure the currency of backup media and that vital records required to support the DR Plan are kept offsite.
Human Resource Manager	Organize orientation programs for new hires and coordinate DR training with Organization DR Coordinator. Maintain currency of personal contact list and ensure offsite backup.
Emergency Response Manager	Conduct evacuation drills and Fire and Safety briefings. Maintain Emergency Response Procedures.

22.7 Authorization

22.7.1 Plan Review and Approval

The Organization DR Coordinator is responsible for coordinating the review of the plan. The DR Plan should be reviewed twice a year. The IT Head is responsible for approving the DR Plan.

22.7.2 Authority to Invoke DR Plan

In the event of a major disaster impacting IT ability to provide services, in scenarios as per 1.3.1, the IT Head or his designated backup is authorized to invoke the DR Plan.

22.8 Authority/References

This *{IT organization name}* DR Plan complies with the *{Organization name}*'s DR Planning policy version # as follows:

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- The organization shall develop a DR Planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours
- The procedures for execution of such a capability shall be documented in a formal DR Plan and shall be reviewed at least annually and updated as necessary
- All personnel responsible for target systems shall be trained to execute DR procedures
- The plan procedures, recovery capabilities, and personnel, including the recovery team and users, shall be tested at least once a year to identify any weaknesses in the recovery capability and effectiveness

The {system name} DR Plan also complies with the following regulatory and business unit policies:

- Any other applicable national policies should be added
- Any other applicable organizational policies should be added

22.9 Record of Changes

Modifications made to this plan since the last printing are as follows:

Record of Changes			

22.10 Business Impact Analysis

Business Impact Analysis, or BIA, is a key step in the DR planning process. The results from a BIA enable the {IT organization name} to identify the requirements and establish recovery priorities to minimize business impact following a major disaster impacting IT.

The BIA report should contain three key components:

- Identify business impact
- Identify critical resources requirement
- Develop IT recovery priorities

22.10.1 Critical Business Functions

No	Critical Business Functions	Description	Potential Loss (\$)				
			2 to 6	6 to 8	8 to 24	24 to 48	Prolong Outage > 30 days
1							

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

No	Critical Business Functions	Description	Potential Loss (\$)				
			2 to 6	6 to 8	8 to 24	24 to 48	Prolong Outage > 30 days
2							
3							

Based on quantifiable potential loss, if incurred for a specified outage duration, the Organization DR Coordinator can identify applications services, servers, reports, desktops, printers and phone requirements and develop recovery priority.

22.10.2 IT Resource Requirements and Recovery Priority

Hrs	CF No.	Applications	Servers	Reports	Desktop/ Printers	Phone	Others
2 to 6							
6 to 8							
8 to 24							
24 to 48							

22.11 Disaster Recovery Strategy and Activities

22.11.1 Recovery Strategy

- Servers/ Applications recovery
- Describe the deployment of technology to enable recovery of business applications/servers to meet the recovery objectives (e.g. tape backup and restoration for lower recovery priority and data replication to achieve shorter recovery capability)
- Desktop recovery support
- Describe any desktop recovery arrangement/ solution.

22.11.2 Recovery Activities

The activities can be categorized into the following stages:

- Response
- Notifications and Damage Assessment Phase
- Activation Phase

- Mobilization Phase
- Recovery
- Re-synchronization
- Resumption
- Return to Normal Operations Phase

22.11.3 Notification and Damage Assessment Phase

This phase addresses the initial actions taken to detect and assess the damage inflicted by a disruption to {*system name*}. Based on the assessment of the event, the plan may be activated by the Organization DR Coordinator.

In an emergency, the {*Organization name*}’s top priority is to preserve the health and safety of its staff before proceeding with the Notification and Activation procedures.

Contact information for key personnel is located in Appendix {*XYZ*}. The notification sequence is listed below:

The first responder is to notify the Organization DR Coordinator. All known information must be relayed to the Organization DR Coordinator.

The Technical Manager is to contact the Damage Assessment Team Leader and inform him/her of the event. The Organization DR Coordinator is to instruct the Team Leader to begin assessment procedures.

The Damage Assessment Team Leader is to notify team members and direct them to complete the below assessment procedures to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the Damage Assessment Team is to follow the outline below.

22.11.4 Damage Assessment Procedures

Detailed procedures should be outlined to include activities to determine the cause of the disruption, potential for additional disruption or damage, affected the physical area and status of physical infrastructure, the status of IT equipment functionality and inventory, including items that will need to be replaced, and estimated time to repair services to normal operations.

- Upon notification from the Organization DR Coordinator, the Damage Assessment Team Leader is to ...

The Damage Assessment Team is to

- Alternate Assessment Procedures:

Upon notification from the Organization DR Coordinator, the Damage Assessment Team Leader is to ...

- The Damage Assessment Team is to

When Damage Assessment has been completed, the Damage Assessment Team

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- The leader is to notify the Organization DR Coordinator of the results.
The Organization DR Coordinator is to Evaluate the Results and Determine whether the DR Plan is to be Activated and if Relocation is Required
Based on Assessment Results, the Organization DR Coordinator is to Notify Assessment Results to Civil Emergency Personnel (e.g. police, fire) as appropriate

22.11.5 Activation Phase

The DR Plan is to be activated if one or more of the following criteria are met:

- *{system name}* will be unavailable and cannot be recovered locally for more than xx hours as specified in 1.3.2
- Facility and major infrastructure are damaged and will be unavailable for more than xx hours
- Other criteria, as appropriate

The IT Head or designated backup is authorized to activate the DR Plan.

22.11.6 Mobilization Phase

When IT Head activates the plan, the Organization DR Coordinator is to activate the call tree to mobilize the recovery team.

The activities in this phase include:

- Activate Call Tree to mobilize the recovery team
- Inform team members to respond and relocate to the alternate site
- Notify offsite vendors (if applicable)
- Activate off-site backup tapes/vital records retrieval
- Inform business units of the decision and regularly provide a status update

22.12 Recovery Phase

This section provides procedures for recovering the application at the alternate site, whereas concurrent efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the *{system name}* at the Alternate Site. Procedures are outlined for each required team. Each procedure should be executed sequentially as presented to maintain well-organized recovery operations.

22.12.1 Recovery Goal (RTO 6 to 8 hours)

State the first recovery objective as determined by the BIA. Each team responsible for executing a function to meet this objective must state the team name and list its respective procedures.

{team name}

- Team Recovery Procedures

{team name }

- Team Recovery Procedures

22.12.2 Recovery Goal (RTO 8 to 24 hours)

State the second recovery objective as determined by the BIA. Each team responsible for executing a function to meet this objective must state the team name and list its respective procedures.

{team name }

- Team Recovery Procedures

{team name }

- Team Recovery Procedures

22.12.3 Recovery Goal (RTO 24 to 48 hours)

State the remaining recovery objectives as determined by the BIA. Each team responsible for executing a function to meet this objective must state the team name and list its respective procedures.

22.13 Return To Normal Operations

This section discusses activities necessary for restoring {system name} operations at the {*Organization name*}’s original or new site. When the computer centre at the original or new site has been restored, {*system name*} operations at the {*alternate site*} must be transitioned back.

The goal is to provide a seamless transition of operations from the {*alternate site*} to the computer centre.

22.13.1 Original or New Site Restoration

Procedures should be outlined for each necessary team to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

{team name }

- Team Resumption Procedures

{team name }

- Team Resumption Procedures

22.14 Concurrent Processing

Procedures should be outlined for each necessary team to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it functions correctly and the DR system is shut down gracefully.

{team name }

- Team Resumption Procedures

{team name }

- Team Resumption Procedures

22.15 Plan Deactivation

Procedures should be outlined for each necessary team to clear the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information.

Materials, equipment, and backup media should be properly packaged, labelled and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

{team name }

- Team Testing Procedures

{team name }

- Team Testing Procedures

22.16 Testing Strategy

The objective of testing the DR Plan is to evaluate whether or not the DR Plan is capable of recovering one or more business-critical processes to functionality within the defined RTO and RPO. At the end of the day, the DR test provides a high level of assurance for the business owners with minimal associated costs and no disruption of services.

Annually, Organization DR Coordinator shall coordinate with the recovery team, supporting vendors and users to conduct DR tests.

22.16.1 Test Scope

The DR test objective is to test the recovery procedures simulating a total data centre site failure. The scope of the test is to cover both online and batch services that support critical business processes, which are identified during the BIA. In addition, the Call Tree Notification test should be performed as a routine exercise to validate the currency of the Personnel Contact list and Vendors Contact list.

22.16.2 Test Approach

An annual simulation test will be performed to test Data Centre DR.

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

The integrated test will be performed on major changes that invalidate the DR recovery plan. This must be done within three months of any change.

Desktop recovery plan tests must be performed as and when changes are made. This must be carried out within three months of the changes.

22.16.3 Successful Test Criteria

The key successes of a DR test criteria are:

- Meet RTO
- Verify recovery capability through users validation
- Effective mobilization of recovery team within 2 hours
- Consistency of maintaining up-to-date recovery procedures

22.17 Awareness and Training Strategy

The main objective is to create awareness of the DR processes and procedures so that all staff is updated and trained on all recovery procedures on a regular basis.

22.17.1 Approach

For a training program to be effective, it must address the following major points:

- All key personnel who are involved in DR should understand the policies and procedures laid out in the plan
- All employees who need to know the procedure to follow when a disaster occurs
- Employees' know-how on the use of disaster management equipment in DR
- Personnel understands their roles and responsibilities in DR

22.17.2 Process

New Employee Orientation Program

All new employees should attend a briefing session on the organization's DR Plan and the expectation of each employee during a disaster situation

Posters and Notices

To raise the awareness of DR process, the Organization DR Coordinator should publish and put up posters and notices of available DR courses, dates of DR exercises, names of participants of DR exercises, recognition from Executive Management on the successful execution of DR exercises onto organization notice-boards and the intranet website. With these publicity channels, the awareness of DR activities will increase, and staff will know their

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

effort in DR Planning and maintenance is well appreciated by the management.

❑ Pre-Drill Training

Organization DR Coordinators and Technical Manager to conduct pre-test briefings to recovery team on DR procedures and new updates.

22.18 Schedule for Review

The following review is to be carried out to ensure the currency of the DR Plan and procedures:

Procedures Review	Frequency	Responsible Party
DR Plan Review	Semi-Annual	Organization DR Coordinator
DR Servers Recovery Procedures Review	Semi-Annual	Technical Manager
Review DR Test Procedures	Semi-Annual	Organization DR Coordinator
Emergency Response Procedures	Annual	Appointed Safety Officer

For effective and compliance with the DR Plan, the following assessments will be performed:

Assessment	Frequency	Responsible Party
Business Impact Analysis	Semi-Annual	Organization DR Coordinator
Personnel Contact List/ Call Tree Review	Quarterly	HR Manager
Vendors Contact List	Quarterly	Technical Manager
Insurance	Annual	IT Head
DR Budget	Annual	IT Head
Business DR Requirement Review	Annual	Organization DR Coordinator
DR Vendor Contract /SLA Review	Annual	Organization DR Coordinator
DR Capacity Review	Annual	Technical Manager

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Assessment	Frequency	Responsible Party
Vital Records and Backup List Review	Quarterly	Media & Vital Records Manager
Equipment inventory Review	Annual	Data Centre Manager

22.19 Plan Appendices

The appendices included should be based on system and plan requirements. Examples are as follows:

- Personnel Contact List
- Vendor Contact List
- Equipment inventory and Specifications
- SLAs and Memoranda of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related DR Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan

23 Appendix G: DR Planning Project - Major Activities / Milestones

23.1 Explanation

In a typical DR Project, the major project milestones or activities should include the following breakdowns of activities. Although the activities are listed sequentially for easy reading, some of these activities may be undertaken concurrently if there are no interdependencies between the activities.

23.2 Project Management

- Preparing and submitting the project proposal to management to justify the project's need and request resources and budget to run the project.
- Establishing the preliminary DR project planning team whose task is to consolidate information and define requirements for the Request For Proposal (RFP) for the services
- Establishing the DR project team structure – defining individual roles and responsibilities, including a list of project deliverables and timeline; a formal periodic management progress update on the development of the DR project plan
- Drawing up the RFP for the acquisition of DR Planning services
- Briefing and issuing the RFP to DR vendors and service providers
- Evaluating the respective RFP responses and shortlisting vendors
- Obtaining management approval to award the RFP to the chosen DR vendor or service provider
- Commencing the project with a kick-off meeting with the various team members

23.3 Risk and Analysis Review

- Identifying all potential risks, both localized and global (if the organization is supporting overseas operations) and evaluating the probability of happenings

23.4 Business Impact Analysis

- Establishing the impact of risk(s) of the business operations; regarding service availability, loss of revenues, loss of critical business information, legal and social liabilities, and impact on business reputation

23.5 DR Strategy

- Identifying the most appropriate recovery strategy based on the nature of business, risk, and tolerable downtime
- Seeking management's approval in adopting the proposed recovery strategy and implementation of the DR Plan

23.6 Plan Development

- Establishing a formal DR Plan development project team structure consisting of business and technical operations representatives.
- Briefing all parties involved in the DR Plan on the how and why the recovery strategy is selected and solicit commitment from them to developing and supporting the DR Planning project.
- Defining the roles and responsibilities, project deliverables and schedules for the development of the DR Plan.
- Defining the following structure and workflow:
 - Roles and responsibilities for all DR team members.
 - DR call tree.
 - Reporting and Escalation.
 - Activation of DR site.
 - Recall of offsite backup.
 - Business applications recovery priority list.
- Drawing up the
 - Inventory list of business applications, hardware, and software.
 - Detailed recovery processes for each of the hardware, software and business applications.

23.7 Testing and Exercising

- Establishing the exercising and testing method for verifying the effectiveness of the DR Plan, processes and procedures.
- Developing relevant test scenarios, test cases and the expected results.
- Conducting briefing and walk-through sessions in the test scenario and test cases for all staff who need to be involved in the test.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

- Documenting all the test results and conducting post-test review meetings to refine and improve the DR Plan.
 - Proposing changes and improvements to the DR Plan.
-

23.8 Program Management

- Establishing the process and procedures for controlling, maintaining and distributing the up-to-date DR Plans to all relevant Executive Management and DR team members.
 - Evaluating and accepting proposed changes or improvements by the DR team and updating the DR Plan.
 - Replacing all outdated DR plans with the updated copy and destroying the outdated copy.
 - Establishing awareness programs and the training roadmap cum schedule for Executive Management, DR team members and all other staff of the organization
-

23.9 Project Completion

- Handing over the complete set of DR Plan to the DR operation and management team
- Reporting to management upon project completion

24 Appendix H: DR Site - Selection & Evaluation Checklist

24.1 Explanation

This checklist provides the reader with some of the key pointers for selecting and evaluating a reliable and secure installation suitable for a DR site. However, these key pointers are not meant to serve as mandatory requirements. The reader may vary these pointers accordingly to his/her respective organization's needs.

Item	Description	Please Tick	
1	Equipment Room	Yes	No
1.1	Access		
1.1.1	Secure with lock and key		
1.1.2	Accessible by authorized personnel only		
1.2	Housekeeping		
1.2.1	Are there any combustible materials in the room?		
1.2.2	Are the combustible materials stored in metal or fire-retardant cabinets?		
1.2.3	Are waste materials removed from the room immediately after any work is completed?		
1.2.4	Is there a policy restricting eating, drinking and smoking?		
2	Electrical Power	Yes	No
2.1	Is there a provision for dual power feeds from different power grids?		

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Item	Description	Please Tick	
2.2	Has the commercial power been tested for spikes, surges, brownouts, noise and other deficiencies that may affect the performance of electrical equipment?		
2.3	Do the electrical grounding meet vendor specifications and local and international standards and regulations?		
2.4	Backup Power for the Facility		
2.5	Are backup power generators installed for emergency power generation?		
2.6	Can the emergency power run continuously for 48 hours?		
2.7	Are the power generators secure and accessible only to authorized personnel?		
2.8	Is emergency lighting available for use during a power failure?		
2.9	Can the environment control system function during a power failure?		
2.10	Are circuit breakers marked and easily accessible to authorized personnel?		
2.11	Are there separate circuit breakers for communications and other equipment?		
2.12	Are uninterruptible power systems installed to provide temporary emergency power before cut-over to power generators?		
2.13	Does the setup conform to local and international electrical regulations on specifications and codes?		
2.14	Is the emergency power generation system tested periodically or at least once a year?		
3	General Building Facilities & Condition	Yes	No

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Item	Description	Please Tick	
3.1	Is the non-electrical piping marked and labelled according to local and international regulations and specifications?		
3.2	Are the environmental conditions (temperature and humidity control) checked and regularly maintained at preset specifications by building maintenance personnel?		
3.3	Does the fire-suppression system conform to local and international fire and safety regulations and standards?		
3.4	Are fire-suppression systems tested periodically or at least once a year?		
3.5	Are there smoke and water detection systems installed?		
3.6	Do the smoke and water detection systems conform to local and international standards and regulations?		
3.7	Does the facility use raise flooring?		
3.8	What is the floor loading capacity?		
3.9	Are there separate cabling systems for electrical power and communication cables?		
3.10	Are the cabling systems only accessible to authorized personnel?		
4	Communications Equipment		
4.1	Are the communications equipment installed in secure enclosures within the equipment room?		
4.2	Is access to the secure enclosures restricted to authorized network and communications personnel?		

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Item	Description	Please Tick	
4.3	Are there policies implemented for the maintenance and testing of communications equipment?		
4.4	Are critical software and information (like routing tables, and firewall policies) backed up periodically and before major network software and hardware changes?		

25 Appendix I - A Sample Questionnaire for Conducting Business Impacts Analysis Interviews

25.1 Explanation

This document serves as a guide to the Organization DR Coordinator in customizing and conducting BIA interviews with various Business Owners of each of the IT application systems.

S/No	Headings	Description/Explanation
1. COVER SHEET		
	Your Name	Name of business unit representative
	Job Title	Job title of the person completing the form
	Business Unit	Name of Business Unit
	Approved by / Signature	Name of Head of Business Unit & Signature
2. IDENTIFICATION OF CRITICAL BUSINESS FUNCTIONS		
Critical Business Function		
2.1	Function Number	<ul style="list-style-type: none"> The acronym for each function and its serial number. This function number is used as a shorter form of identification and a cross-reference to the rest of the document. For example, "HR" is the acronym for Human Resource Department and the function number "HR 1" is Critical Business Function (CBF) Number 1 for HR Department.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/No	Headings	Description/Explanation
2.2	Name of Function	<ul style="list-style-type: none"> Name of critical business function. State a name or identifier (of up to 3 words). Note that the number of functions is usually not expected to exceed 15. "Nice to have"/"convenience functions" should be omitted during the final submission. <p>List the critical business functions that must be carried out in your business areas for acceptable service to be maintained for internal and external customers.</p>
2.3	Description	<ul style="list-style-type: none"> For this exercise, a function is defined as an activity or a group of activities that delivers a product or discrete service. Highlight only the end result and <u>not</u> details of all the processes which enable the function to be completed. Use only one line to describe each function. Start the description with an action <u>verb</u>, e.g. Grant limits, Administer loans, Monitor outstanding transactions.
Business Impact		
2.4	Impact Hard/Soft	<ul style="list-style-type: none"> Hard Impact: Direct Financial Impact Soft Impact: Indirect Financial Impact or Non-Financial Impact
	Total (\$) Impact	What would the total financial impact be on your business unit if you did not carry out this function for seven calendar days?
	How is Impact Quantified?	Describe how this figure is made up, focusing on the most important items. For example, there could be contractual penalties, interest claims, missed business opportunities, loss of commission, etc.
Hard Impact		
	Direct Financial <ul style="list-style-type: none"> Revenue Additional Direct Cost 	<ul style="list-style-type: none"> The financial impact if your entire business unit ceases to function for the next seven days. This entry aims to determine the financial impact on your organization if the function is unavailable. It should be an estimate, and if you cannot provide an accurate answer, please indicate the loss of revenues expected, e.g. \$500,000.
Soft Impact		

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/No	Headings	Description/Explanation
	Indirect Financial impact <ul style="list-style-type: none"> • Overtime • Contractual Penalties • Other 	<p>The indirect financial impact is a loss deemed a “potential” loss, usually a projected loss amount. There is no immediate financial payment required.</p> <p>Examples are:</p> <ul style="list-style-type: none"> • Interest claims for late payments • Fines for not meeting statutory obligations • Other contractual penalties
	Non-financial Impact	<p>This is self-explanatory and requires a descriptive answer. The question is, “Would this non-financial impact apply to you?”</p> <p>Examples are:</p> <ul style="list-style-type: none"> • Loss of license • Loss of good external goodwill • Loss of business/customers • Cash flow problems • Loss of efficiency • Unmanageable back-logs • Loss of financial/management control • Loss of management visibility - without systems, management cannot see where the business is going • Customer relationship • Legal/statutory requirements • Degradation of service • The integrity of operational/historical data - how confident are you that recovered data files will be up-to-date?
2.5	Quantification	The amount of the direct financial impact in local currency, for one week. Please state the period if it is not one week.
2.6	How hard impact is quantified	Provide the workings or basis for computing the amount of loss. For example, \$20,000 is received per day multiplied by a 2% interest payment for an overdraft.
3. RESOURCES USED TO CARRY OUT CRITICAL FUNCTIONS DURING A CRISIS		
3.1	Function Number	Cross-reference to the function number from 2.1.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/No	Headings	Description/Explanation
3.2	No of staff (Min Qty)	<p>Number of staff</p> <ul style="list-style-type: none"> Staff may have overlapping functions and may perform more than one function. Indicate the minimum number of staff needed. Double counting will occur and is acceptable. This number is rationalized as a business unit once the non-critical functions are excluded. <p>Note: If staff are critical (i.e. no overlapping or alternates available), you may want to highlight the names of the staff and their functions.</p>
3.3	<p>Tel (Min Qty)</p> <p>Answer: Y or N</p>	<ul style="list-style-type: none"> Indicate the <u>minimum</u> number of handsets required to perform the function. Note that these handsets may also be required for other functions. <p><u>Note:</u> There may be duplication in the telephone handsets between functions. A review to finalize the total number "Total" should be conducted once the list is completed.</p>
3.4	<p>Vital Records</p> <p>Answer: Y or N</p>	<p>Do you have vital records? e.g.</p> <ul style="list-style-type: none"> Original documents in hard copy Unique documents Reference or other manuals <p>If your answer is "Y", update it immediately in Part 6 of the questionnaire</p>
		<p><u>Original documents in hard copy</u></p> <p>Are your original documents kept as hard copies, such as:</p> <ul style="list-style-type: none"> Customer instructions Applications for Internet Account <p>Note: If such documents exist, business units should consider the methods to reestablish these documents in a disaster.</p>
		<p><u>Unique documents</u></p> <p>This covers unique forms or documents used by the business function, e.g.:</p> <ul style="list-style-type: none"> Property title deeds Customer registration documents Legal documents Maintenance contracts, etc.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/No	Headings	Description/Explanation
	Reference or other manuals Answer: Y or N	This refers to the procedural manuals required, such as: <ul style="list-style-type: none"> Accounting Standards Manual Operating Software Manual
Standalone PC		
3.5	Stand-alone Software (Qty)	How many software applications are "stand-alone"?
3.6	Does PC Data have a backup?	Are your data and stand-alone software backed up?
3.7	Is PC Data kept offsite?	Is your backed-up data kept offsite?
3.8	No. of PCs	The minimum number of PCs needed
3.9	Software of PC (Name of Software)	<ul style="list-style-type: none"> Highlight non-Microsoft Office™ software and non-organization-standard software, such as WordPerfect or StarOffice <p>Default MS Office suites such as MS Word, Excel and PowerPoint are assumed to be available. Also include other LAN-based software, e.g. email.</p>
3.10	Application Software (Name of Application)	<ul style="list-style-type: none"> Name the application systems running on the mainframe or minicomputer used by the business functions. Refer to the list provided by IT Department.
3.11	External info system or services (Name)	<ul style="list-style-type: none"> External information systems or services, e.g. Internet, Reuters, Bloomberg, etc.
3.12	Other resources or special equipment (State Name & Qty)	<ul style="list-style-type: none"> Special equipment is used to support business functions. State the type of equipment, e.g. WAP Phone, Dot Matrix Printer, etc.
4. TIMELINESS OF CRITICAL BUSINESS FUNCTIONS		
4.1	Function	<ul style="list-style-type: none"> Cross-reference to the function number from 2.1
4.2	Normal timescale	<ul style="list-style-type: none"> The timescale for a function to be carried out on a normal day. Refer to the timescale in BIA Questionnaire - The answer is "1" if the time scale is less than 4 hrs, "2" if less than one day, etc.

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

S/No	Headings	Description/Explanation
4.3	Crisis timescale	<p>Would you be able to stretch the timescale for delivering this function during a crisis? Would your customers bear with you?</p> <ul style="list-style-type: none"> • Please make a personal judgment based on a worst-case scenario • Could the function be carried out over a more extended period, possibly using different means during a crisis? • Assume it is not possible to access your office location.
4.4	Function especially critical during or impact scenario	State the specific time, e.g. month-end, year-end, 25th of the month, 4.30 pm daily, etc., whereby the business function is most vulnerable.
5. INTER-DEPENDENCIES (Self-explanatory on the form)		
6. VITAL RECORDS		
6.1	Description of Vital Records	Description of records, e.g. board meeting minutes, any original or unique documents, contracts, files, insurance policies.
6.2	Media Type	Identification of media type, e.g. disks, tapes, reports, forms, microfiche.
6.3	Where held	Identification of storage location of records.
6.4	In Whose Care	Who is responsible for maintaining or keeping the document?

26 Appendix J - A Sample Table of Content of Request For Proposal

26.1 Explanation

This sample table of content provides the general items to be included in the RFP document to acquire DR services.

26.2 Table of Content

- ☐ **1. Introduction**
 - 1.1 Purpose
 - 1.2 Overview

- ☐ **2. Proposal Preparation/Submission**
 - 2.1 Scope of Work
 - 2.2 Request for Proposal (RFP)
 - 2.3 Issues of RFP
 - 2.4 RFP Briefing Session
 - 2.5 Contact for RFP-Related Questions
 - 2.6 Delivery of Proposals
 - 2.7 Modification of Proposals
 - 2.8 Withdrawal of Proposal
 - 2.9 Acceptance or Rejection of Proposals
 - 2.10 Selection of Vendor
 - 2.11 Contract Award
 - 2.12 Timeframe
 - 2.13 Proprietary and Confidential

- ☐ **3. Vendor Instructions**
 - 3.1 General Instructions on Proposal Format
 - 3.2 Special Instructions

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

□ 4. Technical Specifications And Requirements

- Vendor Profile
- Staff and Services
- Hardware, Software & Telecommunication Configuration
- Proposed Pricing
- Terms and Conditions
- Vendor Policies
- Recovery Facility Specifications
- Additional Information

□ 5. Appendix

27 Appendix K: A Sample of DR Test Checklist

27.1 Explanation

The following checklist aims to provide the reader with the sequential steps for conducting a DR test.

DR Test Checklist		
S/N	Items	Status
1.	Design a DR Test Plan <ul style="list-style-type: none">Type of DR test (e.g. checklist test, parallel test)Define test scenarioDefine ObjectiveDefine the Scope of the DR Test	
2.	Establish key success DR test indicators	
3.	Establish Team members <ul style="list-style-type: none">Recovery TeamVendorsUsers	
4.	Survey and review DR requirements	
5.	Validate recovery environment and capacity with vendors	
6.	Confirm the date to conduct the DR test	
7.	Conduct DR Test planning meeting	
8.	Management briefing	
9.	Announce DR Plan to participating users	
10.	Prepare activity plan	
11.	Conduct Pre-Test review meeting	
12.	Conduct DR Test	

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

DR Test Checklist		
S/N	Items	Status
13.	Record and document the test results for audit purposes to track events and measure success.	
14.	Evaluate test results	
15.	Conduct Post-Test reviews	
16.	Consolidate users' test certificates/ feedback	
17.	Consolidate and finalize the Test Report	
18.	Complete the final executive review Present achieved test results against the test objectives: <ul style="list-style-type: none"> • Present strengths and weaknesses • Suggest corrective actions for deviations • Recommend improvements • Assign responsibility to update DR Plan 	
19.	Update DR Plan	

28 Appendix L: A Sample of DR Test Design Template

The following is a sample template to assist the Organization DR Coordinator in designing a DR test:

Test Design Profile for DR Test			
Duration	Purpose	Description	Recommended Practices
Pre DR Test	<u>Definition</u> Objective	<ul style="list-style-type: none">▪ To evaluate the capability of recovering one or more critical business functions in a stipulated disaster scenario▪ To exercise recovery team players in a realistic pressurized environment▪ To demonstrate recovery capability to meet RPO and RTO	<ul style="list-style-type: none">▪ Engage the board of directors▪ Ensure all participating members of the organization understand the objective▪ Organization to agree on RTO and RPO

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Test Design Profile for DR Test			
Duration	Purpose	Description	Recommended Practices
	Type of Test	<ul style="list-style-type: none"> Define test approach, e.g. checklist test, simulation test. 	<ul style="list-style-type: none"> The test must be both practical and realistic
	Scope and Scale	<ul style="list-style-type: none"> Specify business unit, critical services, locations, batch and online, and any specific critical functions, e.g. external interfaces 	<ul style="list-style-type: none"> Be aware of any risks to normal operations
Pre-DR Test		<ul style="list-style-type: none"> Specify business unit, critical services, locations, batch and online, and any specific critical functions, e.g. external interfaces to be included in the test Define the Test date of the transactions 	<ul style="list-style-type: none"> Specify any limitations (Out of Scope). Be aware of any risks to normal operations Specify any limitations (Out of Scope) of the test List of key assumptions made and limitations
	Elements to be tested: Plans People Place Resources	Test Recovery procedures Recovery team, vendors and end-users Recovery Centre, facility Systems, networks, Communications, Facility	<ul style="list-style-type: none"> Engage the management team, board or directors in the plan invocation and management of the activities

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Test Design Profile for DR Test			
Duration	Purpose	Description	Recommended Practices
Pre-DR Test	Success Criteria	<ul style="list-style-type: none"> ▪ Participating recovery team to confirm procedures are accurate ▪ End users' participation and certifications of the test ▪ End-to-end test, including systems and network test ▪ Meet recovery objectives 	<ul style="list-style-type: none"> ▪ Ideally, the key success criteria should be measurable
	<u>Scheduling</u> Time of test/schedule	<ul style="list-style-type: none"> ▪ Indicate the date to conduct the test ▪ The start and end times of the test 	<ul style="list-style-type: none"> ▪ Develop a DR test activity plan.
	Duration	<ul style="list-style-type: none"> ▪ Maximum of 2 hours 	<ul style="list-style-type: none"> ▪ Minimize potential risks or inconveniences to customers.
	Frequency (mandatory/desirable)	<ul style="list-style-type: none"> ▪ Annually ▪ Or any major changes affecting the recovery plan 	<ul style="list-style-type: none"> ▪ Major changes affecting the recovery plan must be retested ASAP. ▪ The organization should develop a DR test policy ▪ The major deficiency must be retested.
	Budget for Testing	<ul style="list-style-type: none"> ▪ Identify internal cost 	

**Business Continuity Management Specialist Series:
A Manager’s Guide to Implement Your IT Disaster Recovery Plan**

Test Design Profile for DR Test			
Duration	Purpose	Description	Recommended Practices
		<ul style="list-style-type: none"> Identify expenses to be incurred (e.g. vendors charges) 	
DR Execution	<u>Execution/Monitoring</u> Controllers/Marshals	<ul style="list-style-type: none"> Manage DR activity schedule Manage users testing Manage problem incident 	<ul style="list-style-type: none"> Coordinate, track and control scheduled activity Document activity schedule
Post-DR Test	<u>Document</u> Documentation (ready to be audited) – track events and degree of success	<ul style="list-style-type: none"> Prepare Post DR Test report Consolidate Test records for archival Consolidate test certifications from users Update DR Plan 	<ul style="list-style-type: none"> Include Key Success indicators Archive test records/reports as test evidence for audit purposes
	<u>Review/Measure</u> Post-Mortem Meeting	<ul style="list-style-type: none"> Yes, immediate debrief (in some instances, there may be a need for a more thorough review meeting some days later) 	<ul style="list-style-type: none"> Conduct Post Test review within two weeks. Review key lessons learned
	<u>Report/Output</u> Post-Test Actions (documented) – linking into Maintenance /reporting	<ul style="list-style-type: none"> Record the outcome of the standard assessment proforma and document remedial actions required (with responsibilities and target dates) 	

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Test Design Profile for DR Test			
Duration	Purpose	Description	Recommended Practices
	<u>Maintenance/Follow-Up</u> Make amendments to planning as required	<ul style="list-style-type: none"> ▪ If appropriate, amend the plan(s) and where their remedial actions requirement negate earlier test result(s), arrange appropriate re-test(s) 	

29 Appendix M: Frequently Asked Questions

29.1 What is DRP?

DR Planning refers to the dynamic development of a coordinated recovery strategy for IT systems (major application or general support system), operations, and data after a disruption. The planning process requires seven steps: develop a DR Planning policy; conduct the business impact analysis (BIA); identify preventive controls; develop recovery strategies; develop DR Plan; test and exercise the plan and train personnel; and maintain the DR plan.

29.2 What is the difference between the various plans?

What are the differences between a DR Plan, a Business Continuity Plan, a Business Resumption Plan, a Continuity of Support Plan, an Incident Response Plan and an Occupant Emergency Plan?

Organizations require a suite of plans to prepare themselves for the response, continuity, recovery and resumption of business processes and IT systems in a disruption.

Each plan has a specific purpose and scope. However, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following fundamental descriptions.

A BC plan addresses sustaining business functions and the IT systems that support those business processes during and after a significant disruption. A Business Recovery (BR) Plan documents the resumption procedures of the organization's business processes at an alternate site. Unlike a BCP, a BRP does not address sustaining operations during the disruption. A DR Plan is an IT-focused plan designed to restore the operability of the target system, application or computer facility at an alternate site after a significant and usually catastrophic disaster. BC and BR plans provide an IT system's recovery and resumption procedures. However, this type of plan is broader in scope than DR Planning because it includes procedures for recovering a system resulting from minor disruptions that do not necessarily require relocation to an alternate site.

An Incident Response Plan establishes procedures to enable security personnel to identify, mitigate, and recover from cyber attacks against an organization's IT system(s). An Occupant Emergency Plan (OEP) provides directions for facility occupants to follow in an emergency situation threatening the health and safety of personnel, the environment or property. Careful coordination must be maintained between plan developers to

ensure that their policies and procedures complement one another. Any changes in one plan, system, or process must be communicated to plan developers of associated systems and processes.

29.3 What is the connection between RM and DRP?

Risk management (RM) encompasses a broad range of activities to identify, control and mitigate risks to an IT system. Risk management should prevent or reduce the likelihood of damage by implementing security controls to protect a system against natural, human and technological threats. Risk management also should encompass actions to reduce or limit the consequences of threats if they successfully disrupt a system. These measures form the basis for DR Planning because the measures are developed in anticipation of a possible event and executed after that event has occurred.

29.4 Into what phase of the SDLC should DRP be incorporated?

Although DR Planning is associated with activities occurring in the operation/maintenance phase, DR measures should be identified and integrated into ALL phases of the System Development Life Cycle (SDLC). Incorporating DR Planning into the SDLC reduces overall DR Planning costs, enhances DR capabilities, and reduces impacts on system operations when the DR Plan is implemented.

29.5 What is the first step I need to take before writing a DR Plan?

The first step in the DR planning process is to develop a DR Planning Policy supported by Executive Management. This policy should define the organization's overall DR objectives and establish the organizational framework and responsibilities for IT DR Planning. The policy statement should also address roles and responsibilities. The policy should be supported with procedures covering training requirements, the frequency of backups, offsite storage shipments, plan exercises, testing, and maintenance.

29.6 Which DR solutions should be implemented to ensure availability?

The BIA, the second step in the DR Planning process, is central to determining what recovery strategies should be implemented to ensure availability. The BIA enables the Organization DR Coordinator to characterize the system requirements fully, processes, and interdependencies to determine DR requirements and priorities. The BIA should be developed with input from all associated system owners, end-users, and internal and external interconnected system partners. Critical resources for accomplishing the IT system's mission(s) should be identified through data calls with these contact points. Possible impacts attributed to the unavailability of these resources over time and across associated systems and processes can then be determined, leading to sequencing the

recovery of the resources based on potential impacts. Thus, the resource requirements and recovery prioritization will form the basis for developing appropriate DR solutions.

29.7 What type of alternate site should I choose?

The type of alternate site should be determined through the BIA. The alternate site choice must be cost-effective and match the availability needs of the organization's IT systems. Thus, if a system requires 100 per cent availability, then a Hot Site might be the right choice.

However, if the system can allow a day of downtime, a Cold Site might be a better option.

29.8 How far should the alternate site be from the primary site?

The distance between an alternate site or offsite storage facility from the primary site should be determined by the scope of the potential threat being considered rather than a specific distance. The Organization DR Coordinator should use the risk assessment to determine the geographic area, accessibility requirements, security requirements, environmental conditions, and cost factors necessary to select a safe and practical offsite facility.

29.9 When an event occurs, who should be notified?

Notification procedures must be outlined in the Continuity Plan. The Organization DR Coordinator should determine who should be notified if a disruption occurs to the IT system and in what sequence they should be contacted. Parties notified typically include the system owners, users and major associated application and general support systems. External entities that might be interconnected to the IT system should also be included in the notification procedures. The design of a call tree will assist the sequence and responsibilities of executing notifications to appropriate contacts.

29.10 What is the Resumption Phase?

The Resumption Phase is implemented after the Recovery Phase is executed. In this phase, procedures are carried out to restore the original facility and IT system to normal operating conditions. For example, using the original site or system is not feasible due to extensive damage. Actions should be taken during the Resumption Phase to procure and prepare a new facility or IT system. When the original or new site and system are ready, recovery activities are terminated, and normal operations are transferred back to the organization's facility.

29.11 How often should my DR Plan be tested?

Testing helps to evaluate the viability of plan procedures, determine the ability of recovery staff to implement the plan, and identify deficiencies in the plan. Testing should occur annually and when significant changes are made to the IT system, supported

business process(s), or the DR Plan. Each element of the DR Plan should be tested individually to confirm the accuracy of recovery procedures and the overall effectiveness. Test and exercise schedules should be stated in the DR Plan policy statement.

29.12 How often should my DR Plan be updated?

An up-to-date plan is essential for successful DR plan operations. As a general rule, the plan should be reviewed for accuracy and completeness at least annually and upon significant changes to any element of the DR plan, system, business processes supported by the system, or resources used for recovery procedures. Deficiencies identified through testing should be addressed during plan maintenance. In addition, elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently.

Maintenance schedules should be stated in the DR Planning policy statement.

29.13 How are DR Plan and its solutions coordinated?

In addition to integrating DR Planning into the SDLC, DR Planning should be coordinated with network security policies. System security controls can help to protect against malicious code or attacks that could compromise system availability closely coordinated with the incident response procedures. In addition, the DR Plan should be closely coordinated with other emergency preparedness plans related to the IT system, interconnected systems, and business processes.

30 Index

A

Alternate Sites Options · 112
Alternate Sites Recovery Strategy · 113
Application Data
 Data Type Classifications · 93
Asynchronous Replication
 Replication · 103
Awareness and Training · 162
Awareness Programs · 164

B

BCM Planning Methodology · 18
Budget · 51
Business Continuity Management · 16, 17
Business Continuity Management (BCM) Specialist Series · 16
Business Impact Analysis · 18, 76
Business Impacts Analysis · 214
Business Recovery Teams · 133

C

Catch-up Data
 Data Type Classifications · 95
Change Management Process · 159
Checklist Test · 153
Cloud computing · 33
Cloud deployment model · 33
Cloud Services Model · 37
Cluster
 Resilient Storage Implementation · 107
Cold Site · 113
 Alternate Sites Recovery Strategy · 113
Community Cloud
 Cloud deployment model · 35
Control Measures · 74
Crate and Ship · 117
Critical Data
 Data Criticality Classification · 96
Cutover Test · 154

D

Damage Assessment · 143

Data Backup and Electronic Vaulting · 100
Data Backup Media · 174
Data Backup Strategy · 97, 99
Data Backups
 Data Protection and Recovery Strategy · 99
Data Criticality Classification · 96
Data Mirroring
 Mirroring · 104
Data Recovery Process · 109
Data Replication
 Replication · 104
Data Safety Classifications · 95
Data Type Classifications · 93
Data Types · 94
Database Data
 Data Types · 94
Database Replication
 Replication · 104
Database Shadowing
 Mirroring · 105
DBMS Data Log Backup
 Data Backup Strategy · 98
Dedicated Site
 Alternate Sites Options · 112
 Alternate Sites Options · 112
Differential Backup
 Data Backup Strategy · 97
Disaster Recovery · 27
Disaster Recovery as a Service
 DRaaS · 42
Disaster Recovery Life Cycle · 135
Disaster Recovery Plan · 27
Disaster Recovery Planning · 27
Disaster Recovery Teams · 132, 133
Disk Mirroring
 Mirroring · 105
DR Management Team · 133
DR Plan Test Cycle · 153
DR Planning Methodology · 18
DR planning team · 48
DR Site - Selection & Evaluation Checklist · 210
DR steering committee · 48
DR Test Checklist · 222
DR Test Design · 224
DRaaS · 43
Drivers for Disaster Recovery · 23

E

Electronic Vaulting

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

Data Backup and Electronic Vaulting · 101

F

Frequently Asked Questions · 229
Full Backup
 Data Backup Strategy · 97
Full InterruptionTest · 154

H

Hot Backup
 Types of Data Backup Strategy · 98
Hot Site · 114
 Alternate Sites Recovery Strategy · 114
Hybrid Cloud
 Cloud deployment model · 35

I

Impact Area · 64
Incremental Backup
 Data Backup Strategy · 97
Infrastructure as a Service
 Cloud Services Model · 38
Infrastructure Data
 Data Type Classifications · 93
Insurance · 73

L

Lost Data
 Data Type Classifications · 95

M

Mirror Backup
 Types of Data Backup Strategy · 98
Mirroring · 104
Mobile Site · 115
 Alternate Sites Recovery Strategy · 115

N

Network Attached Storage · 107, 182
 Resilient Storage Implementation · 107
Non-critical Data
 Data Safety Classifications · 97
Non-Database Related Data
 Data Types · 95
Notification Contact List · 142

O

Online Backup
 Data Backup Strategy · 97
Orphan Data
 Data Types · 94
Outsourcing · 73

P

Paper Test · 153
Parallel Test · 154
Physical Offsite Vaulting
 Data Backup and Electronic Vaulting · 100
Plan Activation · 144
Plan Development · 18, 131
Plan Distribution Process · 160
Plan Maintenance · 159
Platform as a Service
 Cloud Services Model · 38
Private Cloud
 Cloud deployment model · 34
Program Management · 19, 158
Project Management · 18, 44
Public Cloud
 Cloud deployment model · 34

R

Reciprocal Site
 Alternate Sites Options · 112
 Alternate Sites Options · 113
Recover · 136
Recovery as a Service
 Cloud Services Model · 39
Recovery Objectives · 78
Recovery Point Objective · 78
Recovery Procedures · 145
Recovery Strategy · 18, 91, 92, 99, 112
Recovery Strategy phase · 91
Recovery Time Objective · 79
Reduce · 136
Redundant Arrays of Independent Disks
 Resilient Storage Implementation · 106
Remote Journaling
 Mirroring · 105
Remote Mirroring
 Mirroring · 105
Remote Tape Vaulting
 Data Backup and Electronic Vaulting · 101
Replication · 101
 Data Protection and Recovery Strategy · 99
Request for Proposal · 119
Request For Proposal · 220
Resilient Storage Implementation · 106
Response · 136
Resume · 137
Re-sync · 137, 145

Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan

Return · 137
Risk Acceptance · 71
Risk analysis · 59
Risk Analysis · 60
Risk Analysis & Review · 18
Risk Analysis and Review · 59
Risk assessment · 59
Risk Assessment · 62
Risk Assessment Workflow · 60, 61, 62
Risk Avoidance · 70
Risk Reduction · 71
Risk Transference · 71
Risk Treatment · 70, 71
Risk treatment, · 59

S

Safe
 Data Safety Classifications · 96
Sensitive Data
 Data Safety Classifications · 96
Service Level Agreement · 116
Software as a Service
 Cloud Services Model · 38
Storage Area Network · 107, 182
 Resilient Storage Implementation · 107
Storage Virtualization · 182
Synchronous Replication
 Replication · 102
System Data
 Data Type Classifications · 94
Systems Backup Strategies · 92

T

Table of Contents of DR Plan · 190
Test Scenario · 152
Testing & Exercising · 19
Testing and Exercising · 151
Traditional Disaster Recovery · 40
Training Programs · 165

U

Unsafe
 Data Safety Classifications · 95

V

Virtualization
 Resilient Storage Implementation · 106
Vital Data
 Data Criticality Classification · 96

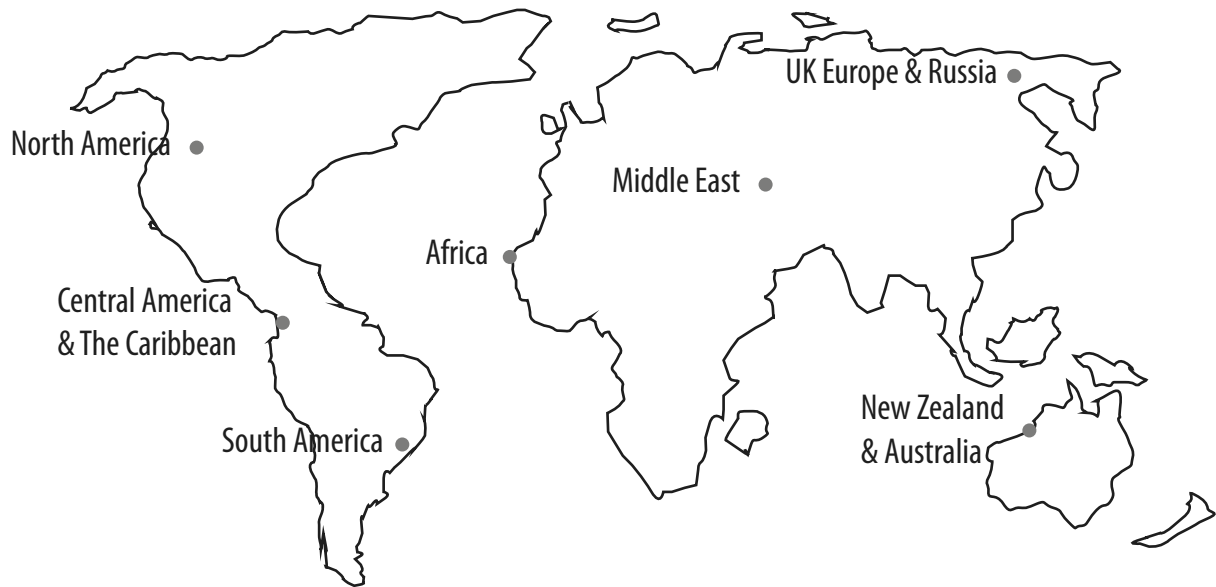
W

Walkthrough Test · 153
Warm Site · 114
 Alternate Sites Recovery Strategy · 114

**Business Continuity Management Specialist Series:
A Manager's Guide to Implement Your IT Disaster Recovery Plan**

A decorative graphic element consisting of a grid of small white dots on a black background, located on the left side of the page below the photograph.

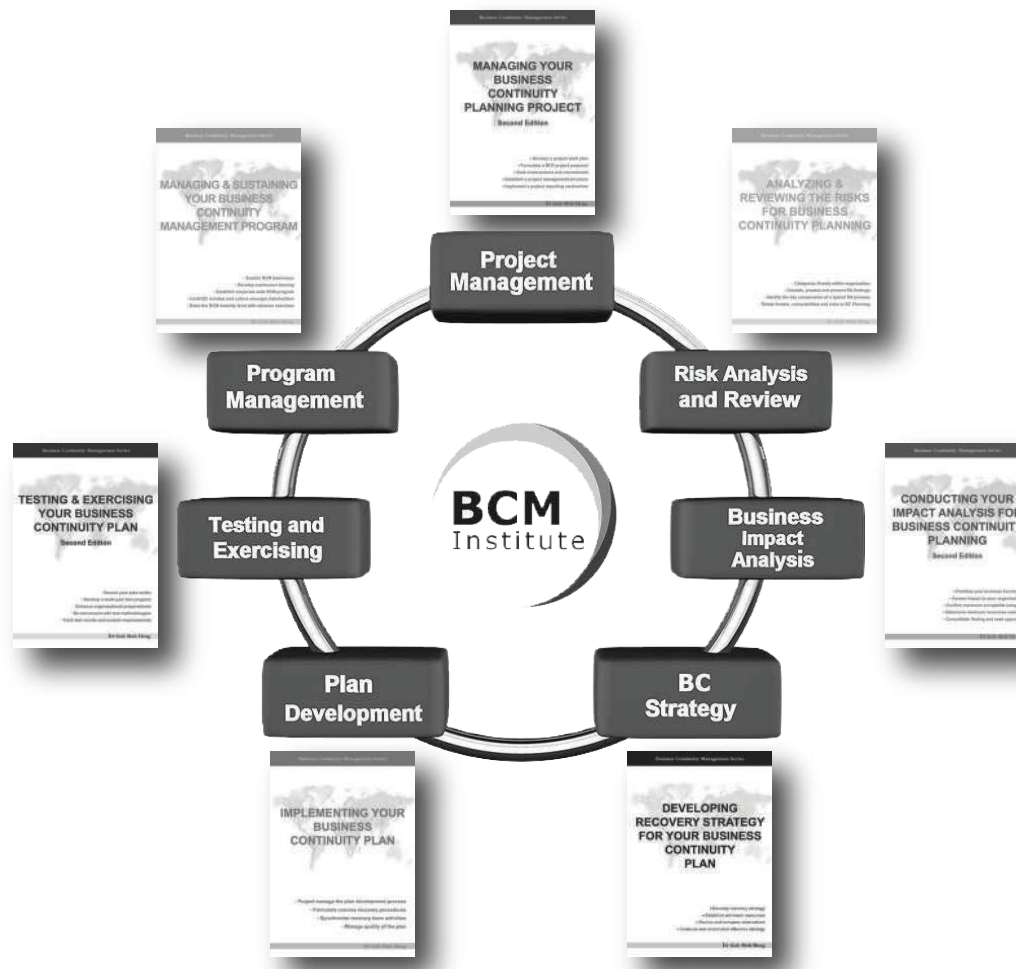
ABOUT BCM INSTITUTE



Countries with professionals certified by BCM Institute

- We are a global convergence of thought leadership in ISO 22301 BCMS Audit, Business Continuity, Crisis Management, Crisis Communication and IT Disaster Recovery.
- Global Professional Development and Qualification developed by Technical Experts and Thought Leaders
- Largest Continuity Training and Certification Organization in Asia Pacific
- Governed by Education, Examination and Certification Committees
- Delivered by Industry Practitioners, Professionals and Peers
- Attended by Professionals, Practitioners, Consultants, Auditors, Officials from all industry sectors of over 1000 Organizations and Multi-National Corporations (MNC)

Education	Professional Development	Thought Leadership
Conducting and administering courses and examinations	Provide a career path and a common body of knowledge for business continuity and disaster recovery professional	Organizing conferences and seminar events. Publishing technical and research papers.



BCM Planning Methodology

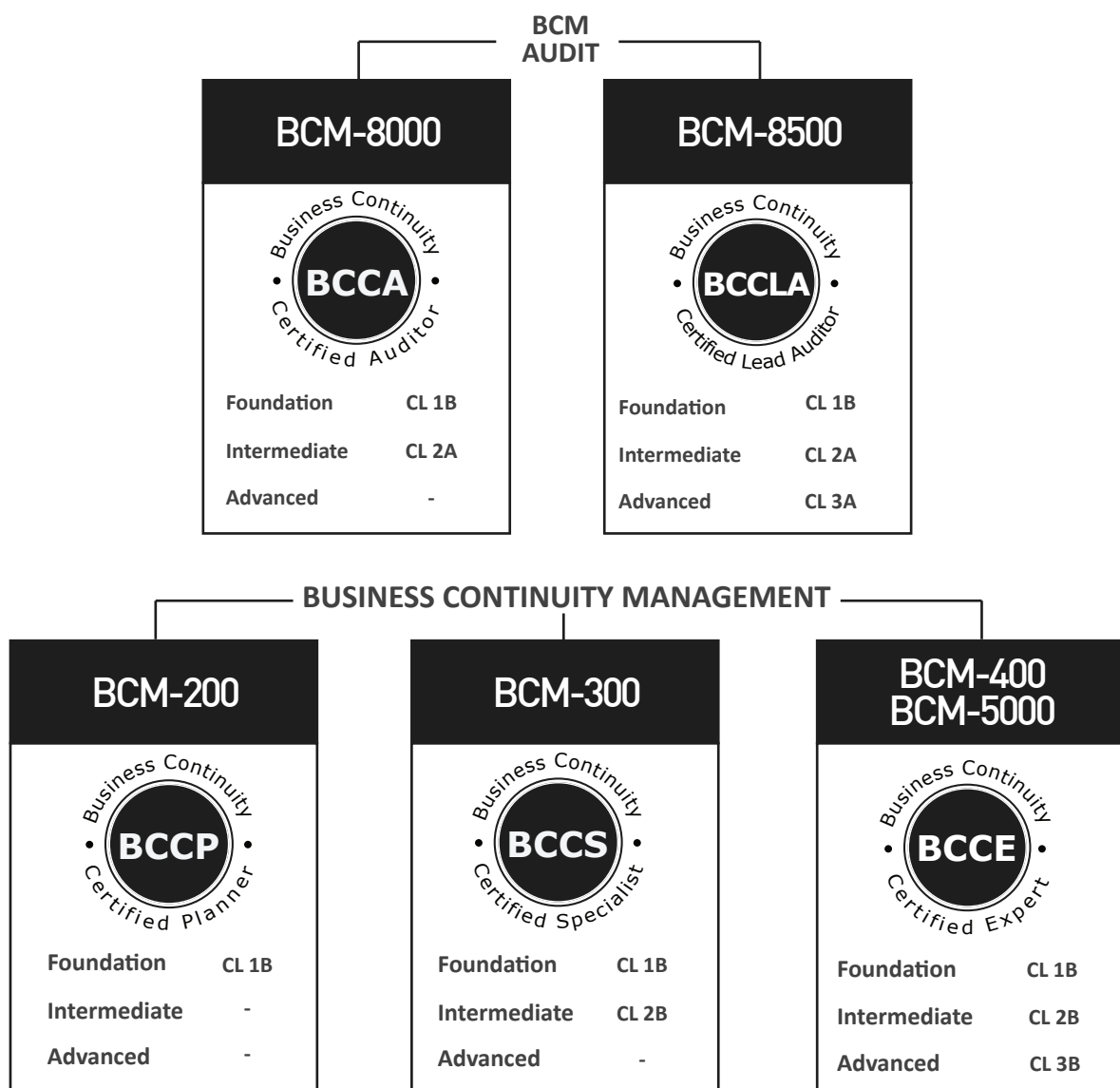
BCM Institute’s planning methodology’s strength lies in its practical and proven usage by professionals and practitioners worldwide. First developed by technical experts, the methodology today can be seen throughout international standards. One key aspect of BCM Institute’s implementation methodology is that it has been modulated for ease of transference and multiple standards implementation within a single core framework. This methodology is based on 7 areas of the Body of Knowledge, also known as, BOKs. To support the learning and development of our methodology, each BOK is learned through various Competency Levels.

Certification Types and Levels



The BCM Institute’s Certification programs support the community in BCM Audit, Business Continuity Management (BCM), Crisis Management (CM), Crisis Communication (CC), IT Disaster Recovery (IT DR) and are designed to ensure a consistency high standard of professional practice and recognize individuals’ competencies in the BCM sphere. The certification program requirements and eligibility standards are applied fairly, impartially, and consistently. The certification program may grant certification independently of a candidate’s membership or non-membership in any organization, association or other groups.

Participants are expected to be competent in the respective competency level (CL) upon completion of the preparatory course.



Certification Types and Levels



CRISIS MANAGEMENT (CM)

CM-200



Foundation	CL 1C
Intermediate	-
Advanced	-

CM-300



Foundation	CL 1C
Intermediate	CL 2C
Advanced	-

**CM-400
CM-5000**



Foundation	CL 1C
Intermediate	CL 2C
Advanced	CL 3C


CRISIS COMMUNICATION (CC)

CC-200



Foundation	CL 1CC
Intermediate	-
Advanced	-

CC-300



Foundation	CL 1CC
Intermediate	CL 2CC
Advanced	-


**CC-400
CC-5000**



Foundation	CL 1CC
Intermediate	CL 2CC
Advanced	CL 3CC


IT DISASTER RECOVERY PLANNING (DRP)

DRP-200




Foundation	CL 1D
Intermediate	-
Advanced	-

DRP-300



Foundation	CL 1D
Intermediate	CL 2D
Advanced	-

**DRP-400
DRP-5000**



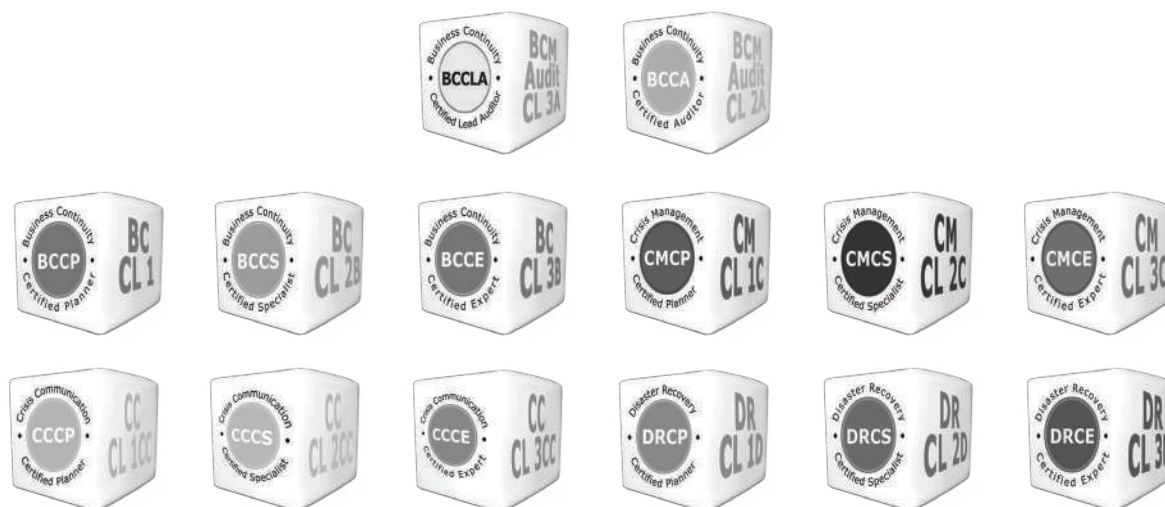
Foundation	CL 1D
Intermediate	CL 2D
Advanced	CL 3D

Criteria	Candidate Must :
Education	Complete the prescribed preparatory courses
Examination	Meet and successfully pass the prescribed examinations in accordance to the preparatory course level or desired certification levels
Experience	Possess the necessary assessable experience in accordance to the desired certification levels
Continuing Education Hours	Continue to develop the skills and knowledge to maintain the credentials of the certification

The Institute is governed by independent committees, supported by its published set of BCM Body of Knowledge (BCMBoK). The BCMBoK serves as the basis for the competency program for the assessment and qualification of professionals in BCM Audit, Business Continuity Management (BCM), Crisis Management (CM), Crisis Communication (CC) and IT Disaster Recovery (IT DR).

As part of the requirements for certification, professionals are required to demonstrate their knowledge through examinations at levels prescribed by BCM Institute's Education and Examination Committees. Skills and capabilities are assessed through verifiable experience presented in the application for certification form.

Qualified candidates are presented certification credentials at the discretion of the BCM Institute's Certification Committee. Candidates are advised to enrol in the BCM Institute's preparatory courses prior to undertaking the prescribed examination. To maintain the use of credentials, certified members must demonstrate active involvement in BCM through annual declaration of continuing education hours.



Building Blocks

The Competency Level, or CL, forms a framework and becomes a set of building blocks for BCM Institute's training and certification requirement.

It consists of three levels: Foundation (CL 1), Intermediate (CL 2) and Advanced (CL 3).

Knowledge Domain

The education and certification for BCM are:

- A** BCM Audit
- B** Business Continuity Management
- C** Crisis Management
- CC** Crisis Communication
- D** IT Disaster Recovery

The arrangement of the tiers represents the increasing level (CL 1, CL 2 and CL 3) of specificity and specialization of the BCM Audit skills, BCM skills, CM skills, CC skills, IT DR skills and their knowledge content. This content is mainly applicable to participants attending the Institute's education and certification program.

A AUDIT

The domains for the BCM Audit courses are:

- CL 2A: Intermediate is taught in the BCM-8000 or related course (preparing for the BCCA certification examination).
- CL 3A: Advanced is in BCM-8500 or related course (preparing for the BCCLA certification examination).

For more information please visit <http://bcmpedia.org>

CL 2A, [http://www.bcmpedia.org/wiki/CL_2A:_Intermediate_\(Audit\)](http://www.bcmpedia.org/wiki/CL_2A:_Intermediate_(Audit))

CL 3A, [http://www.bcmpedia.org/wiki/CL_3A:_Advanced_\(Audit\)](http://www.bcmpedia.org/wiki/CL_3A:_Advanced_(Audit))



B BUSINESS CONTINUITY MANAGEMENT

- The domains for the BCM courses are:
 - CL 1B: Foundation will be taught in the foundation course (BCM-200 course preparing for the BCCP certification exam).
- CL 2B: Intermediate (BCM-300 preparing for the BCCS certification examination).
- CL 3B: Advanced (BCM-400/ BCM-5000 preparing for the BCCE certification examination).

For more information please visit <http://bcmpedia.org>

CL 1B, [http://www.bcmpedia.org/wiki/CL_1B:_Foundation_\(BC\)](http://www.bcmpedia.org/wiki/CL_1B:_Foundation_(BC))

CL 2B, [http://www.bcmpedia.org/wiki/CL_2B:_Intermediate_\(BC\)](http://www.bcmpedia.org/wiki/CL_2B:_Intermediate_(BC))

CL 3B, [http://www.bcmpedia.org/wiki/CL_3B:_Advanced_\(BC\)](http://www.bcmpedia.org/wiki/CL_3B:_Advanced_(BC))



C CRISIS MANAGEMENT

- The domains for the CM courses are:
CL 1C: Foundation will be taught in the foundation course (CM-200 course preparing for the CMCP certification exam).
- CL 2C: Intermediate (CM-300 preparing for the CMCS certification examination).
- CL 3C: Advanced (CM-400/ CM-5000 preparing for the CMCE certification examination).

For more information please visit <http://bcmpedia.org>
CL 1C, [http://www.bcmpedia.org/wiki/CL_1C:_Foundation_\(CM\)](http://www.bcmpedia.org/wiki/CL_1C:_Foundation_(CM))
CL 2C, [http://www.bcmpedia.org/wiki/CL_2C:_Intermediate_\(CM\)](http://www.bcmpedia.org/wiki/CL_2C:_Intermediate_(CM))
CL 3C, [http://www.bcmpedia.org/wiki/CL_3C:_Advanced_\(CM\)](http://www.bcmpedia.org/wiki/CL_3C:_Advanced_(CM))



CC CRISIS COMMUNICATION

- The domains for the CC courses are:
CL 1CC: Foundation will be taught in the foundation course (CC-200 course preparing for the CCCP certification exam).
- CL 2CC: Intermediate (CC-300 preparing for the CCCS certification examination).
- CL 3CC: Advanced (CC-400/CC-5000 preparing for the CCCE certification examination).

For more information please visit <http://bcmpedia.org>
CL 1CC, [http://www.bcmpedia.org/wiki/CL_1CC:_Foundation_\(CC\)](http://www.bcmpedia.org/wiki/CL_1CC:_Foundation_(CC))
CL 2CC, [http://www.bcmpedia.org/wiki/CL_2CC:_Intermediate_\(CC\)](http://www.bcmpedia.org/wiki/CL_2CC:_Intermediate_(CC))
CL 3CC, [http://www.bcmpedia.org/wiki/CL_3CC:_Advanced_\(CC\)](http://www.bcmpedia.org/wiki/CL_3CC:_Advanced_(CC))



D IT DISASTER RECOVERY

- The domains for the disaster recovery courses are:
CL 1D: Foundation will be taught in the foundation course (DRP-200 course preparing for the DRCP certification exam).
- CL 2D: Intermediate is taught in the DRP-300 course (preparing for the DRCS certification examination).
- CL 3D: Advanced is in DRP-400/5000 course (preparing for the DRCE certification examination).

For more information please visit <http://bcmmedia.org>




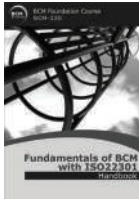


















CL 1D, [http://www.bcmmedia.org/wiki/CL_1D:_Foundation_\(DR\)](http://www.bcmmedia.org/wiki/CL_1D:_Foundation_(DR))

CL 2D, [http://www.bcmmedia.org/wiki/CL_2D:_Intermediate_\(DR\)](http://www.bcmmedia.org/wiki/CL_2D:_Intermediate_(DR))

CL 3D, [http://www.bcmmedia.org/wiki/CL_3D:_Advanced_\(DR\)](http://www.bcmmedia.org/wiki/CL_3D:_Advanced_(DR))



Certification

	Fundamental	Intermediate	Advance
ISO22301 Auditor		 <p>Course Code: BCM-8000</p> 	 <p>Course Code: BCM-8500</p> 
ISO22301 BCMS	 <p>Course Code: BCM-200</p> 	 <p>Course Code: BCM-300</p> 	 <p>Course Code: BCM-400 BCM-5000</p> 
Crisis Management	 <p>Course Code: CM-200</p> 	 <p>Course Code: CM-300</p> 	 <p>Course Code: CM-400 CM-5000</p> 
Crisis Communication	 <p>Course Code: CC-200</p> 	 <p>Course Code: CC-300</p> 	 <p>Course Code: CC-400 CC-5000</p> 
IT Disaster Recovery	 <p>Course Code: DRP-200</p> 	 <p>Course Code: DRP-300</p> 	 <p>Course Code: DRP-400 DRP-5000</p> 

Competency-Based

INITIATING BCM PROGRAM



Course Code:
BCM-410

IMPLEMENTING BCM MANUAL



Course Code:
BCM-420

ASSESSING RISK AND BUSINESS IMPACT REQUIREMENT



Course Code:
BCM-310

DEVELOPING BUSINESS CONTINUITY STRATEGIES AND PLANS



Course Code:
BCM-320

TESTING AND EXERCISING BUSINESS CONTINUITY PLAN



Course Code:
BCM-330

EXECUTING CRISIS MANAGEMENT AND BUSINESS CONTINUITY PLAN



Course Code:
BCM-340

MANAGING BCM PROGRAMME



Course Code:
BCM-450

PROVIDING MANAGEMENT REVIEW AND OVERSIGHT



Course Code:
BCM-460

BCM Planning Book series

Dr Goh Moh Heng



MANAGING YOUR BUSINESS CONTINUITY PLANNING PROJECT



ISBN :
978-981-05-9767-2

Year Release :
2008

2nd Edition

ANALYZING & REVIEWING THE RISKS FOR BUSINESS CONTINUITY PLANNING



ISBN :
978-981-05-9215-8

Year Release :
2008

CONDUCTING YOUR IMPACT ANALYSIS FOR BUSINESS CONTINUITY PLANNING

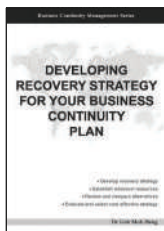


ISBN :
978-981-05-9654-5

Year Release :
2008

2nd Edition

DEVELOPING RECOVERY STRATEGY FOR YOUR BUSINESS CONTINUITY PLAN



ISBN :
981-05-0670-8

Year Release :
2005

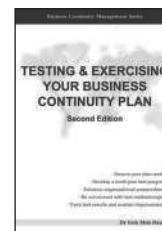
IMPLEMENTING YOUR BUSINESS CONTINUITY PLAN



ISBN :
981-04-8169-1

Year Release :
2004

TESTING & EXERCISING YOUR BUSINESS CONTINUITY PLAN



ISBN :
981-05-5848-1

Year Release :
2006

2nd Edition

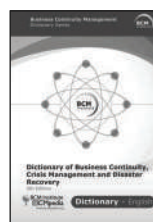
MANAGING & SUSTAINING YOUR BUSINESS CONTINUITY MANAGEMENT PROGRAM



ISBN :
981-05-4392-1

Year Release :
2007

DICTIONARY OF BUSINESS CONTINUITY, CRISIS MANAGEMENT AND DISASTER RECOVERY

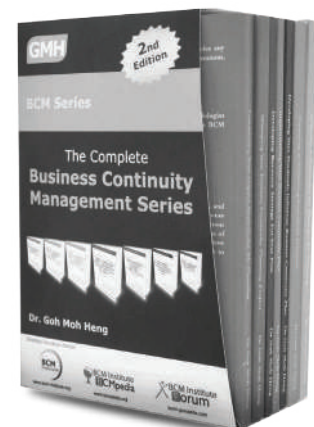


ISBN :
978-981-09-1156-0

Year Release :
2015

5th Edition

The Complete Business Continuity Management Series



BCM Specialist Book series

Dr Goh Moh Heng



A MANAGER'S GUIDE TO
ISO 22301 STANDARD FOR
BCM SYSTEM



ISBN :
978-981-07-2512-9
Year Release :
2014

A MANAGER'S GUIDE TO
BRITISH STANDARD BS25999
FOR BCM



ISBN :
978-981-08-9260-9
Year Release :
2012

A MANAGER'S GUIDE TO
SINGAPORE STANDARD SS540
FOR BCM



ISBN :
978-981-05-4299-3
Year Release :
2011

A MANAGER'S GUIDE TO
AUDIT & REVIEW YOUR
BCM PROGRAM



ISBN :
978-981-05-4300-6
Year Release :
2014

A MANAGER'S GUIDE TO
IMPLEMENT YOUR IT
DISASTER RECOVERY PLAN



ISBN :
978-981-04-5975-8
Year Release :
2009

A MANAGER'S GUIDE TO
IMPLEMENT YOUR
INFECTIOUS DISEASE BC PLAN



ISBN :
981-05-5227-0
Year Release :
2015

A MANAGER'S GUIDE TO
IMPLEMENT YOUR CRISIS
COMMUNICATIONS PLAN



ISBN :
978-981-09-2671-7
Year Release :
2015

A MANAGER'S GUIDE TO
IMPLEMENT YOUR CRISIS
MANAGEMENT PLAN



ISBN :
978-981-07-4836-4
Year Release :
2015

A MANAGER'S GUIDE TO
IMPLEMENT YOUR SUPPLY
CHAIN BCM PLAN



ISBN :
978-07-2513-6
Year Release :
2015

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR AIRPORTS



Year Release :
2015

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR EDUCATIONAL INSTITUTIONS



Year Release :
2015

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR HOTEL



Year Release :
2016

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR INSURANCE COMPANIES



Year Release :
2016

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR FACILITIES



Year Release :
2017

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR MANUFACTURING SECTOR



Year Release :
2017

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR HOSPITAL



Year Release :
2017

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR BUSINESS PROCESS OUTSOURCING



Year Release :
2017

INDUSTRY GUIDE TO BUSINESS CONTINUITY MANAGEMENT FOR FINANCIAL INSTITUTION



Year Release :
2017



Meet The Experts

www.worldcontinuitycongress.com

Meet- The- Expert (MTE) travels across the globe as an interactive peer to peer and Subject Matter Expert dialogue platform to address both business and technical areas surrounding the Business Continuity Management (BCM), Crisis Management (CM), Crisis Communication (CC) and Disaster Recovery Planning (DRP) and Crisis Management (CM) issues at a localized perspective. Presented regularly as a complimentary seminar, MTE is an opportunity for novices and industry professionals to gain and share knowledge with Subject Matter Experts and industry practitioners.



World Continuity Congress

www.worldcontinuitycongress.com

The World Continuity Congress (WCC) has established itself to be the unparalleled platform for Business Continuity, Disaster Recovery and Crisis Management offering access to some of the most remarkable professionals in the international industry.

The conference has been held annually since 2000 and brings together professionals from around the world into key cities across Asia. WCC is honoured to be the platform of choice for Senior Management and practitioners from a wide array of industries participating in this dynamic congress.

A black and white photograph showing a group of people in business attire networking and talking in a hallway or event space.

World
Continuity Congress

16 April 2013
Resorts World Sentosa,
Singapore

BUILDING RESILIENCE THROUGH CRISIS MANAGEMENT AND COMMUNICATION



Business Continuity Management Specialist Series

This series of books aims to equip the reader with the skill set needed as a specialist to assist organizations to survive any unexpected crisis with expected results in continuing business and IT operations.

A Manager's Guide to Implement Your IT Disaster Recovery Plan

This book prepares the reader to apply the framework, principles and methodologies for implementing an IT disaster recovery plan. It uses the writer's experience to enable you to deploy an internationally recognized DR planning methodology with a strong foundation in conceptualizing, developing and maintaining an effective and efficient DR plan.

This innovative text aims to provide its readers with a structural and procedural approach to develop a DR plan for the entire IT infrastructure and services that are required for its critical business applications. It also includes practical DR guidelines, considerations, practices and samples that is beneficial for DR practitioners to facilitate and manage the DR planning process.

Learn How To :

- Design an DR planning project applicable to a wide range of organizations.
- Put up a management proposal for implementing a DR plan.
- Identify the drivers and benefits of having the DR plan.
- Appreciate the different degrees of impact that disasters can have on business application and operations.
- Evaluate an organization's needs against recovery strategy options and technical considerations.
- Document the strategy into a DR plan.
- Verify the effectiveness and correctness of the DR plan.
- Maintain and update the DR plan to reflect its applicability during any unexpected disaster at any time.

