

Contents

Chapter 1:	Building a Disaster Recovery Plan—The Need	1
	The Need	3
	Plan for All Types of Disasters	11
	Reasons for Planning	13
	Let’s Get Started	17
	Phase 2: Definitions and Risk Mitigation	26
	Phase 3: Server Criticality and Recovery Strategies	33
	Phase 4: Develop the Plan	40
	Phase 5: Validate the Recovery Plan	43
	Summary	46
Chapter 2:	Vulnerability Assessment & Risk Analysis	49
	Site Vulnerability Assessment	50
	Vulnerability Assessment Summary	73
	Performing a Risk Analysis	74
	Summary	85
Chapter 3:	Conducting a Business Impact and	
	Recoverability Analysis	87
	Starting the Business Impact Analysis	89
	Tangible Costs	90
	Intangible Costs	94
	Identifying Mission-Critical Functions	96
	Outage Impact	100
	Recovery Time Objective vs. Recovery Point Objective.	104
	Shifting Focus for Return on Investment (ROI)	115
	The Process of the BIA.	116
	Summary	121
Chapter 4:	Critical Server Ranking	123
	Classifying Systems for Recovery Priority	124
	Mission-Critical Only, Please	125

	Rank Your Data Backup Priorities	127
	Backups, and Recovery Time and Point Objectives	129
	Critical Systems Definition, A List.	132
	Critical Systems Definition, B List.	134
	Is Email Mission-Critical?	135
	Hardware Requirements for Mission-Critical Servers	135
	Summary	136
Chapter 5:	Building Recovery Strategy Requirements	139
	The Disaster Recovery Challenge	140
	Guidelines for Selecting Recovery Strategies	141
	Market Trends	144
	Recovery Strategies	146
	Data Center Recovery Solutions	150
	Determine the Level of Business Resiliency	
	You Want to Achieve	156
	Overall Site Restoration Strategy Sample	158
	Summary	159
Chapter 6:	Backup and Recoverability.	161
	Plan for Data Recovery	162
	10 Issues for the Administration of Backups.	167
	Checklist for Backup and Recovery	174
	Backup Media Management	176
	How Much to Back Up for Disaster Recovery.	185
	Backup Recovery and Media Services (BRMS)	186
	A Simple Save Strategy	192
	Save More with Save-While-Active	195
	Richard's Backup Solution	198
	Backups for Planned Maintenance Windows	199
	IBM's Virtual Tape Solution (VTL)	200
	Duplicate Your Removable Media	203
	Restoration Commands	204
	The BRMS System Recovery Report	207
	How the System Restores Access Paths	209
	Backing Up and Recovering a Domino Server.	209

	Hardware Management Console (HMC)	213
	Summary	214
Chapter 7:	Your Business Value of Systems Availability.	217
	High Availability—Take the High Road	219
	Recovery on Your High-Availability Investment	220
	Is Your H/A Truly High Availability?	232
	IBM’s Capacity Backup Offering	248
	Summary	250
Chapter 8:	Vital Records and Critical Data Offsite Storage	251
	Vital Record Management	253
	Offsite Storage Considerations.	268
	Choosing an Offsite Storage Provider	271
	Summary	273
Chapter 9:	Building Your Teams	275
	Selecting Candidates: Pick Me! No, Don’t Pick Me!	277
	When There Is Loss of Life or Missing People	281
	Building Your Recovery Teams.	284
	How to Work Together	289
	The IT Recovery Management Team.	293
	The IT Technical Recovery Team	298
	The Network Team	300
	The Hardware Recovery Team	301
	Application Recovery Team	302
	Facility Recovery Team	303
	Replacement Equipment	304
	Disaster Recovery Preparedness	304
	Administrative Responsibilities	305
	Care for Your Recovery Teams During a Disaster	305
	The Team’s Meeting Place	310
	Summary	314
Chapter 10:	Effective Communications	317
	Develop an Employee Call Sheet	319
	Who Do You Contact?	323

	Selecting a Meeting Place for the Command Center. . . .	329
	Facing and Dealing with the Media	334
	Notification Solution Design.	338
	Summary	340
Chapter 11:	How to Develop and Document	
	a Disaster Recovery Plan	341
	Disaster Recovery Plan Development Overview.	342
	Ready, Set, Write the Plan	353
	The Disaster Recovery Plan's Structure	359
	Developing and Writing the Procedures	365
	Disaster Recovery Teams Overview	381
	Summary	389
Chapter 12:	Effective Plan-Activation Procedures	391
	The Disaster-Alert Notification Procedure	393
	First-Alert Response	396
	Hot-site Call-up Procedures	406
	Recalling Tapes from Your Offsite Storage Provider. . . .	412
	Site Restoration Activities	413
	Summary	422
Chapter 13:	The Need for System-Related Documentation	425
	A Change in the i5 Philosophy Silos.	427
	Write It All Down	428
	I Thought Those Backup Tapes Had Everything!	429
	Collecting and Maintaining System Information	431
	The Prtysinf Command	432
	Complete Site Loss versus Server Loss	434
	Summary	441
Chapter 14:	System i5/iSeries Restoration Procedures	443
	Recovery Procedures.	444
	Case Study Sample.	444
	Summary	475

Chapter 15:	System i5/iSeries BRMS Restoration Procedures.	477
	Summary	506
Chapter 16:	Testing Your Disaster Recovery Plan	507
	Practice Just Like the Pros	510
	Satisfy the Need for Testing	511
	The Embarrassment of Testing: What If We Fail?	512
	Open-Book Testing.	514
	Define a Complete Testing Project.	515
	Passive Testing	518
	Active Testing	529
	Disaster Recovery Coordinator Testing Duties.	533
	Introducing Murphy’s Law.	534
	Evaluation of Test Results	535
	Be a Survivor.	536
	Summary	538
Chapter 17:	Plan Maintenance.	539
	Your Plan Design	541
	Implementing a Maintenance Philosophy	542
	Revisit Your Plan—Get into Maintenance Mode.	545
	Change Management.	549
	Summary	560
Chapter 18:	Selecting a Commercial Hotsite Provider	563
	Advance Planning = Hotsite	564
	Internal or External Hotsite?	566
	What to Look for in a Hotsite Provider	567
	Cost Considerations	576
	Summary	581
Chapter 19:	A Family DR Plan.	583
	Disaster Recovery Begins at Home	584
	Emergency Supplies	585
	Practice and Maintain Your Plan	587
	Personal and Family Requirements	588

	Awareness Training.	589
	Information on Family Disaster Plans	589
	Summary	590
<i>Appendix</i>	Sample Documents	591
	Business Impact Analysis Questionnaire.	591
	Operational Priorities.	592
	Operational Impacts	592
	Customer Service	593
	Cash Flow/Revenue	593
	Regulatory (If Applicable)	594
	Increases In Liability.	594
	Vendor Relations	595
	Financial Control/Reporting	595
	Mission Critical IT Applications	596
	Vulnerability	596
	Server Criticality Analysis	597