Index

1-800 telephone service notification, 339
9/11 example, loss of life or missing people during, 281–284

A

A-list recovery strategy for servers, 124, 132–134, 133*t*, 380, 380*t*
access paths, restoration of, 209
access to hotsite, determining ease of, 571–572
accountability for DRP, 18–20
activation procedures for DRP, 391–423, **394**
active testing, 529–532
administrative responsibilities, for team for disaster recovery, 305
air conditioning systems, 52. *See also* humidity levels; temperature levels
alarms, 68–71
alert declaration of potential disaster, 369
alert notification procedure, 393–396
alternate installation devices, 71–72
alternate meeting places, command center and, 330
alternate sites, 154
American Red Cross, 589
Annualized Loss Exposure (ALE), 82–84
antistatic devices, 55
application recovery team, 302. *See also* teams for disaster recovery
assessing damage, 401–404
assessment of established organization, understanding, 350–351
assessment phase of DRP, 348
assumptions of the DRP, 374
audits of disaster preparedness, 14
authority for DRP, 26
authorization list
  for hotsite, 406, **407**, 408–409
  for tape backup access, 412–413, **413**
Auxiliary Storage Pools (ASPs), 127
availability, 39–40. *See also* high-availability servers
avoiding risks, 80
awareness training, 589

B

B-list recovery strategy for servers, 125, 134–135, 134–135*t*, 381, 381*t*
backup, 37–38, 148–150, 149–150*t*, 161–215. *See also* recovery
  access path restoration after, 209
  automation of, 173
  backup lists for Domino and, 213, 213*t*
  backup partitioning and, 235, **235**
  Backup Recovery and Media Services (BRMS) in, 166, 171–172, **171**, 186–192, **186**, **187**. *See also* Backup Recovery and Media Services
  best practices in, 166–167
  Capacity Backup system from IBM and, 248–250, 249*t*
  change-control process integration with, 173–174
  checklist for, 174–175

NOTE: Boldface numbers indicate illustrations; italic t indicates a table

backup, *continued*
- checkpoints and checkpoint images in, 196–197
- CobiT framework for, 167
- control groups for Domino and, 212, 212*t*
- Critical Control Data (CCD) and, 213–214
- customer log sample from, 168–169
- daily incremental, 193–194, 198–199
- data recovery from, 162–167
- Domino Servers and, tips for, 209–213
- elements of System i5 in, **190**–**191**
- failures of, 171
- flexibility of, 142
- full system saves in, 193
- GO SAVE command for, 192–195, 213–214
- Hardware Management Console (HMC) for, 213–214, **214**
- how much to include in, 185
- how often to run, 163
- i5/iSeries restoration, 444
- importance of, 161
- Integrated File System (IFS) and, 209
- lifecycle program for, 169–170
- log review from, 170–171
- media for, 176–184. *See also* tape backups
- monthly strategy for, 193
- nighttime schedule for, 167–169
- orphan data and, 172–173
- planned downtime/maintenance and, 199–200, 224–226, **224**, **225**
- planning for, 169
- priorities for, ranking of, 127–129, 129*t*, 187–192, **188**–**191**
- program temporary fix (PTF) installation and, 199–200
- PRTDSKINF and, 173
- Ragged enhancement for SWA saves in, 198
- RAID disks and, 202
- recovery from, 165–166
- Recovery Point Objectives (RPO) and, 129–132, 131*t*, 164
- recovery strategies for, 204–214. *See also* recovery
- Recovery Time Objectives (RTO) and, 129–132, 131*t*, 164
- regulatory compliance and, 166
- removable media and, duplication of, 203–204
- RESTORE commands and, 204–206, 205*t*
- Restore Object Using BRMS (RSTBRM) in, 212
- Save Changed Objects (SAVCHGOBJ) in, 193–194
- Save Libraries (SAVLIB) in, 194, **199**
- Save Option in, 188–192, **188**, **189**
- Save Security Data (SAVSECDTA) in, 194–195, 198–199, **199**
- save windows in, 163
- save-while-active (SWA) saves in, 195–198, **197**, **198**
- Start Backup Using BRMS (STRBKUBRM) in, 210
- strategy for, 164–165, 192–195
- tape in. *See* tape backup
- technical expertise required for, 174
- technology recovery in, 164–165
- ten key issues in, 167–174
- Virtual Tape Libraries (VTL) in, 200–203, **201**, **203**
- weekly strategy for, 193
- window for, when backups run longer than, 172

backup lists, Domino servers, 213, 213*t*

backup partitioning and, 235, **235**

Backup Recovery and Media Services (BRMS), 186–192, **186**, **187**, 477–506
- backup and, 181
- benefits of, 186–187
- control group in, 192
- control groups for Domino and, 212, 212*t*
- disk configuration build at home system, using Option 3, 487–492, **487**–**491**
- disk configuration build at hotsite, using Option 2, 484–487, **484**, **485**
- Domino Servers and, 210–213, **211**
- elements of System i5 in, **190**–**191**
- Licensed Internal Code restore for, 478–484, 480*t*, **481**–**484**
- media class in, 192
- media identifier in, 192
- media in, 192

operating system restore in, 492–503, **493**–**502**
policies in, 192
prioritizing needs for, 187–192, **188**–**191**
product recovery, 503–505, **503**, **504**
protecting from corruption, 171–172, **171**
resources required for, 478
restoration of, 477–506
Restore Object Using BRMS (RSTBRM) in, 212
Save Option in, 188–192, **188**, **189**
Start Backup Using BRMS (STRBKUBRM) in, 210
system recovery report in, 207, **208**
tape backups and, 260
terminology of, 192
vital records management and, 260
barcode support, vital records management and, 266
basis of DRP, 351–352
battery supplies, 56–57. *See also* uninterruptible power supplies (UPS)
disposing of, 58
benefits analysis, for commercial hotsites, 577–579
blackouts. *See* power outages
brownouts. *See* power outages
building infrastructure, for commercial hotsites, 568–569
building recovery strategy requirements. *See* strategies for recovery
business continuity planning (BCP), 13
Business Impact Analysis (BIA), 30–31, 76, 87–121, 139
consolidate responses to BIA questionnaire for, 118–120
critical IT application identification for, 117
high-availability (H/A) servers and, 220
impact of outage in, assessing costs of, 100–104
intangible cost analysis in, 94–95
interview approach to, in mission-critical function identification, 99–100
IT to verify business data in, 102
labor costs/overtime in, 92–93
late fees and penalties in, 93
legal costs in, 93
mission-critical function identification in, 96–100, 118–120, **119**
objectives of, setting, 116–117
opportunity loss in, 94–95
participants/personnel needed for, 89–90
planned vs. unplanned outages and, impact of, 102–104, **104**
process of, 116–121
productivity losses in, 92–93
questionnaire for, 117, 591–597
Recovery Point Objective (RPO) and, 88, 104–115, **106**, **111**, **113**
recovery strategies and, 34
Recovery Time Objective (RTO) and, 88, 104–115, **106**, **107**, **108**
remedial expenses in, 95
Return on Investment (ROI) and, 88, 105–115, **106**, 115–116
revenue losses in, 91–92
review findings of, 120–121
risk analysis vs., 76
servers and, 124
tangible cost analysis in, 90–93, **91**
validate responses to BIA questionnaire for, 118
vital records management and, 252
workshop approach to, in mission-critical function identification, 97–99

C

call sheets, employee, 319–323, **320**, 339–340
call-up. *See* hotsite, call-up procedures for
cameras, security, 69–71
Capacity Backup system from IBM, 248–250, 249*t*
caring for the team during disaster, 305–310
chain of command established for recovery team, 297–298
challenges of disaster recovery, 140–141
change control process/change management, 549–560. *See also* maintaining the DRP
backup and, integration with, 173–174
company data and, 553–554
design of, 541–542
Disaster Recovery Coordinator's role in, 558–559

change control process/change management, *cont.*
- distribution technology and, 557–558
- documentation and, 556
- hardware and, 550–551
- maintaining the DRP and, 544–545, **545**
- revision tracking in, 560, 560*t*
- software and, 551–553
- vital record management and, 555

changes in i5 philosophy silos, documentation and, 427–428

changes/updates to DRP, 22, 23–24, 42–43

checkpoints and checkpoint images, 196–197

Chief Financial Office (CFO)'s role in DRP, 18

Chief Information Officer (CIO)'s role in DRP, 18

cipher locks, 70–71

clustering of servers, 35

CobiT framework, 167, 253

cold sites, 152–153

command center. *See also* communications
- alternate meeting places for, 330
- assembling team at, 399–400
- equipping, 331–333
- location of, 329–330
- meeting place for, selection of, 329–333, **334**
- rules of communication for, 331
- staffing of, 330

command-center stress, 283–284

commercial hotsite providers, 563–581. *See also* hotsites; off-site storage providers, choosing
- access to, determining ease of, 571–572
- advance planning for, 564–565
- benefits analysis for, 577–579
- building infrastructure of, 568–569
- contract costs for, inclusion and renewals, 579–580
- cost considerations of, 576–581, 578*t*
- electrical power supplies and, 568
- equipment requirements for, 570–571
- experience of, 573
- internal vs. external hotsites and, 566–567, 566–567*t*
- number of customers served by, 572–573
- security of building in, 568–569
- selection criteria for, 567–576
- tendering an offer to, 574–576
- testing access and, 573
- tour of facilities in, 569–570

commitment control in transaction processing, 35

commitment to DRP, 22–24

communications, 317–340, 399. *See also* command center
- 1-800 telephone service notification in, 339
- alternate meeting places for, 330
- employee call sheets in, 319–323, **320**, 339–340
- equipping the command center for, 331–333
- form of, succinct nature of, 325–326
- high-availability (H/A) servers and, 244–245
- importance of, 317–318
- media coverage and, facing and dealing with, 334–337
- media spokesman for, 336–337
- meeting place for command center and, selecting, 329–333, **334**
- notification of personnel in, 327–329, 327*t*
- notification solution design for, 338–340
- official privacy notice for, 323
- phone dialogues in, 326–327
- phone list maintenance for, 339–340
- privacy of contact lists/call sheets used in, 322–323
- Recovery Point Objectives (RPOs) and, 318
- Recovery Time Objectives (RTOs) and, 318
- rules of, 331
- staffing of command center for, 330
- team leaders and members, 287–288
- testing of call-notification process for, 318, **318**
- web site notification in regional disasters and, 338
- who to contact in event of emergency, 323–329, **324**

company data, maintenance and change management in, 553–554

completeness of DRP, 21

compliance. *See* regulatory compliance

comprehensiveness of DRP/recovery strategy, 21–22, 143

connectivity, high-availability (H/A) servers and, 245

container identification tag, **271**

container vaulting, vital records management and, 266
content of DRP procedures, 358–359
contingency planning, 13
continuous systems availability, 234–235
contract costs, commercial hotsites and, inclusion and renewals, 579–580
control group
  BRMS, 192
  Domino, 212, 212*t*
cooling units, portable, 54–55
cooling, 52. *See also* humidity levels; temperature levels
cost, 147
  Annualized Loss Exposure (ALE) in, 82–84
  of commercial hotsites, 576–581, 578*t*
  dollar value benefit and, 225
  of downtime, 31–33, 79, 90–93, **92**, 131–132, 218–219, 220–231
  of DRP, 36–37
  intangible, 94–95
  of labor/overtime, 92–93
  of late fees and penalties, 93
  of legal issues, 93
  opportunity loss as, 94–95
  productivity losses as, 92–93
  of recovery, 143–144
  of remedial expenses, 95
  revenue losses as, 91–92
  tangible, 90–93, **91**
crashes. *See* hardware failure
crisis management phase of DRP, 348–349
Critical Control Data (CCD), 213–214
critical systems in server recovery, 124–125, 132–134
  A-List, 124, 132–134, 133*t*, 380, 380*t*
  B-List, 125, 134–135, 134–135*t*, 381, 381*t*
criticality assessment, server, 33–40. *See also* servers
currency of DRP, 22
Customer Relationship Management (CRM), 217

D

daily incremental backups, 193–194, 198–199
damage assessment following disaster, 401–404
data, maintenance and change management in, 553–554
data center solutions, 150–155
  side-by-side systems and, 236–239, **236**
data recovery, 162–167
database replication, 234–235
DataMirror, 249
death or serious injury, 282
declaration of disaster, 369–370
design of DRP, in maintenance, 541–542
desirable vs. undesirable traits for DR team, 277–280, 277*t*
developing the DRP, 40–43, **41**, 40
device configuration restore, in i5/iSeries restoration, 470–471
diesel and natural-gas generator backups, 61–62
directions and map to hotsite, 409–410, **410**, **411**
Disaster Recovery (DR) defined, 6, 370
Disaster Recovery Coordinator
  maintaining the DRP and, role of, 558–559
  testing the DRP and, role of, 533–534
Disaster Recovery Plan (DRP), 4, 13, 17–26, 341–389, 391–423
  accountability for, 18–20
  activation procedures/process for, 391–423, **394**
  activities encompassed by, 392
  alert declaration of potential disaster in, 369
  alert notification procedure in, 393–396
  assessing current status of, Phase 1, 17–18, **17**
  assessment and initial response phase of, 348
  assumptions of, 374
  authority for, 26
  backup strategies and, 37–38
  basis established for, 351–352
  Business Impact Analysis (BIA) in, 30–31
  changes/updates to, 22, 23–24. *See also* maintaining the DRP
  completeness of, 21
  comprehensiveness of, 21–22
  content of procedures included in, 358–359
  costs of, 36–37
  crisis management phase in, 348–349
  critical systems definition in, A-List, 380, 380*t*
  critical systems definition in, B-List, 381, 381*t*
  currency of, 22
  declaration of disaster in, 369–370
  defining objectives of, 20–22

Disaster Recovery Plan (DRP), *continued*
- definitions for, 369–373
- development and documentation of, 341–389
- development of, Phase 4 in, 40–43, **41**
- disaster defined in, 370
- disaster recovery coordinator's role in, 19
- disaster recovery defined in, 370
- disaster recovery plan defined in, 370–371
- distribution list for, 388, 388*t*
- distribution of, 46
- downtime cost assessment in, 31–33
- DR operations phase in, 349
- end user acceptance of, 45
- established organization of, understanding, 350–351
- executive sponsor for, 19–20
- facilities restoration phase of, 350
- family, 583–590. *See also* family DRP
- first-alert response in, 396–405
  - assessing damage in, 401–404
  - hotsite alerted to disaster in, 400–401
  - initial assessment, verifying disaster in, 396–398
  - notifying personnel in, 404–405
  - personnel status assessment in, 398
  - team assembly at command center in, 399–400
- geographic risks in, 29–30
- high-availability (H/A) servers and, 232–234
- historical risks in, 29
- hotsites defined in, 371
  - authorization list for, 406, **407**, 408–409
  - directions and map to, 409–410, **410**, **411**
  - opening of, 411–412
  - vendor information necessary for, 406
- human error risks in, 30
- initiating, checklist for, 422–423
- introductory text in, 366–367
- IT management team's role in, 371, 382–383, 383*t*
- IT technical recovery team role's in, 383–384, 384*t*
- maintaining, 42–43, 312–314, 539–561. *See also* maintaining the DRP
- mission statement of, 368–369, **369**
- objectives of, 345, 367–368
- overview of development in, 342–353, **343**, **344**
- phases of, 341–342, 346–350, **347**
- planning team for, 24–26, 89–90. *See also* teams for disaster recovery
- prevention defined in, 372
- prevention phase of, 347–348
- primary site restoration team (IT management team) in, 384
- procedures in, developing and writing, 365–381
- recalling tapes from off-site storage provider in, 412–413
- recovery defined in, 372
- Recovery Point Objectives (RPO) in, 32, 36–37, 372
- recovery progression in, 384, **385**, **386**, **387**
- recovery strategies in, 34–37
- recovery team defined in, 372–373
- Recovery Time Objectives (RTOs) defined in, 31, 36–37, 345, 373
- regulatory compliance and, 30
- restoration defined in, 373
- risk assessment for, Phase 2 of, 26–33, **27**. *See also* risk assessment
- sequence of events/timeline for recovery/restoration in, 418–421, **418**, **422**
- server criticality and recovery strategies in, Phase 3 in, 33–40, **33**
- server restoration process in, definition and documentation of, 352
- site restoration activities in, 413–422. *See also* restoration
- software overview in, 376–378, **379**
- staff commitment to, 22–24
- structural attributes of, 345–346
- structure of (in outline form), 359–365
- style of, 357–358
- supported services in, 375–376
- table of contents of, 366
- team overview in, 381–388, **382**, 392–393
- technological risks in, 30
- technology requirements for, 37
- test defined in, 373

testing and recovery validation defined for, 352–353
testing, 44–45, 312–314, 507–538. *See also* testing the DRP
title page of, 365–366
tools to aid in writing, 357–358
types of risk, 29–30
validation of, Phase 5 of, 43–46, **43**
writing of, 353–359

disasters
cost of, 36
death or serious injury in, 282
declaration of, 369–370
definition of, 4–5, **5**
effects of, 8–9, 280
IT impact and, 9–11
loss of life or missing people during, 281–284
types of, planning for, 11–12
who to contact in event of, 323–329, **324**

disk configuration build at home system
Backup Recovery and Media Services (BRMS) and, using Option 3, 487–492, **487**–**491**

disk configuration build at hotsite
Backup Recovery and Media Services (BRMS) and, using Option 2, 484–487, **484**, **485**
i5/iSeries restoration, using Option 2, 451–454, **451**, **452**
i5/iSeries restoration, using Option 3, 454–459, **454**–**458**

disposing of batteries, 58
distributing the DRP, 46, 388, 388*t*, 557–558
distribution list for the DRP, 388, 388*t*
document library restore, in i5/iSeries restoration, 473
documentation, system-related, 425–441, 556
backup tape system and, 429–431
changes in i5 philosophy silos and, 427–428
collecting and maintaining information for, 431–432
detailing and, 428–429
importance of, 426
Intel system information for, 437–440
iSeries/400 system information for, 434–437
network system information for, 440–441
Print System Information (PRTSYSINF) command for, 431, 432–434
site vs. server loss and, 434–441

dollar value benefit, 225
Domino Servers
backup and recovery tips, 209–213, **211**
backup lists for, 213, 213*t*
control groups for, 212, 212*t*
Restore Object Using BRMS (RSTBRM) in, 212
Start Backup Using BRMS (STRBKUBRM) in, 210

doors, 69–71
downtime costs, 31–33, 79, 90–93, **92**, 131–132, 218–219, 220–231
downtime, planned vs. unplanned, 220–231, **221**
DR operations phase of DRP, 349
drop-ship solutions, 152
dry-pipe fire suppression/sprinkler systems, 67–68
DSPLOGBRM, 170

E

earthquakes, 71
e–business, 217
effects of disaster, 8–9, 280
electrical power supplies, 55–62, 568
batteries in, 56–57. *See also* uninterruptible power supplies (UPS)
diesel and natural-gas generator backups for, 61–62
failures in, 56
frequency fluctuations in, 57
harmonic distortion in, 57
highly redundant power supply configuration and, **60**, 61–62
over-voltage conditions in, 56–57
sags/drops in, 56
shock hazards and, 55
spikes in, 56
static and antistatic devices, 55
surge and surge suppression in, 55, 56
under-voltage conditions in, 56–57

electrical power supplies, *continued*
uninterruptible power supplies (UPS) in, 56–62, 568. *See also* uninterruptible power supplies (UPS)
email, as mission-critical application, 135
emergency supplies, 585–587
employee call sheets, 319–323, **320**, 339–340
end-user acceptance of DRP, 45
Enterprise Resource Planning (ERP), 10, 192, 217
environmental controls, vital records management and, 267
equipment
assessing status of, 413–414
hotsite requirements of, 570–571
replacement of, 414–415
equipping the command center, 331–333
essential systems, in server recovery, 124–125. *See also* servers
established organization of DR, understanding, 350–351
evacuation drills, 537–538
evaluating risks, 81–82
executive sponsor of DRP, 19–20
expiry dates, vital records management and, 261
exposure, in risk assessment, 82–84

F

facilities restoration phase of DRP, 350
facility monitoring devices/alarms, 68–69
facility recovery team, 303. *See also* teams for disaster recovery
family DRP, 583–590
awareness training in, 589
documents, 587
emergency supplies for, 585–587
first aid supplies for, 586–587
food supplies for, 586
Hurricane Rita example of, 588–589
information to help create, 589
issues to cover in, 585
maintaining, 587
personal and family requirements for, 588
practice for, 587
water supplies for, 586
Federal Emergency Management Agency (FEMA), 11–12, 589
fences, 69–71
fire drills, 537–53
fire suppression systems, 65–68
pre-action sprinklers in, 68
wet vs. dry pipe systems in, 67–68
first-aid supplies, 586–587
first-alert response, 396–405
assessing damage in, 401–404
hotsite alerted to disaster in, 400–401
hotsite call-up procedures in, 406–412
initial assessment, verifying disaster in, 396–398
notifying personnel in, 404–405
personnel status assessment in, 398
team assembly at command center in, 399–400
flexibility of recovery strategy, 142
flooding. *See* water damage
food supplies, 586
team for disaster recovery and, 306–307
frequency fluctuations, electrical power supplies and, 57
frequency, in risk assessment, 82–84
full-system backups, 193

G

gates, 69–71
geographic risks, 29–30
GO SAVE command, 192–195, 213–214
goal setting for disaster recovery team, 289
grandfather, father, son (GFS) strategy, tape backup media, 262–263, **263**

H

hardware maintenance and change management, 550–551
hardware failure, 4, 12
alternate installation devices and, 71–72
license internal code CD and, 72–73
Hardware Management Console (HMC), 213–214, **214**
hardware recovery team, 301–302. *See also* teams for disaster recovery

hardware requirements for mission-critical servers, 135–136
harmonic distortion, electrical power supplies and, 57
hazardous materials, 69
Health Insurance Portability and Accountability Act (HIPAA), 15, 16, 35, 253
heating systems, 52. *See also* humidity levels; temperature levels
high-availability (H/A) servers, 35–36, 39–40, 143, 145, 217–250, 249*t*
  assessing level of availability in, 231–248
  backup partitioning and, 235, **235**
  Business Impact Analysis (BIA) and, 220
  Capacity Backup system from IBM and, 248–250, 249*t*
  communications needs in, 244–245
  connectivity needs in, 245
  continuous systems availability and, 234–235
  cost justification for, 230–231, **231**
  Disaster Recovery plans and, 232–234
  downtime vs., 218–219, 220–231
  importance of, 219
  iSeries, 249, 249*t*
  maintenance cost benefits for, 226, **226**
  monitoring and maintenance for, 241–243
  Recovery Point Objectives (RPO) and, 231
  Recovery Time Objectives (RTO) and, 231
  replication vs., 234–235
  Return on Investment (ROI) and, 221–231
  side-by-side systems and, 236–239, **236**
  size of target machine in, 239–241, **240**
  target/source compatibility in, 243–244
  testing of, 245–248
  workload balancing cost benefit of, 227–230, **227**, **228**
highly redundant power supply configuration, **60**, 61–62
historical risks, 29
hotsites, 35, 145, 153–154, 371. *See also* commercial hotsite providers
  alerting to disaster, 400–401
  authorization list for, 406, **407**, 408–409
  call-up procedures in, 406–412
  directions and map to, 409–410, **410**, **411**
  internal vs. external hotsites, 566–567, 566–567*t*
  opening of, 411–412
  vendor information necessary for, 406
human error risks, 30
humidity levels, site vulnerability assessment and, 52–54
hurricanes, 71. *See* natural disasters; weather related disasters
HVAC, 52. *See also* humidity levels; temperature levels

I

i5/iSeries restoration
  backup strategy and, 444
  BRMS restoration in, 477–506. *See* Backup Recovery and Media Services
  case study sample of, 444
  device configuration restore in, 470–471
  disk configuration build at hotsite and, using Option 2, 451–454, **451**, **452**
  disk configuration build at hotsite and, using Option 3, 454–459, **454–458**
  library restore, IBM and user (NONSYS), 471–472
    document library, 473
    user library, 472
  LIC restore, 445–450, **447**, **449**, **450**
  operating system restore in, 459–469, **460–467**
  procedures for, 444
  system security rebuild in, 474–475
  user profile restore in, 469–470, **470**
  verification of restore in, 473–474
IBM compliance for DR, 14
impact analysis, 79–80
impact of outages/downtime, 9, 30. *See also* Business Impact Analysis (BIA)
  cost assessment of, 100–104
  planned vs. unplanned, 102–104, **104**
incremental backups, 193–194
Independent Auxiliary Storage Pools (IASPs), 127
individual media vaulting, vital records management and, 267

Information Technology (IT)
  business impact analysis (BIA) and, verifying business data, 102
  disaster's effect on, 9–11
  evolution of importance of, 10–11, 10*t*
infrastructure of commercial hotsites, 568–569
Initialize Tape (INZTAP) command, 177–180, **180**, 182, 259
initial assessment, verifying disaster, 396–398
initial response phase of DRP, 348
injury, serious, 282
installing backups, alternate installation devices for, 71–72
insurance, 84–85
insurance inspection, 415–416
intangible cost analysis, 94–95
Integrated Auxiliary Storage Pools (IASP), 111
Integrated File System (IFS), backup and, 209
Intel system information for documentation, 437–440
internal vs. external hotsites, 566–567, 566–567*t*
interview approach to mission-critical function identification, 99–100
introduction text of DRP, 366–367
IPL, alternate system for, 71–72
iSeries/400 system information for documentation, 434–437
issue identification, in risk assessment/analysis, 78–79
IT management team, 293–298, 371, 382–383, 383*t*. *See also* teams for disaster recovery
IT recovery team personnel, 554–555
IT technical recovery team, 298–300, 383–384, 384*t*. *See also* teams for disaster recovery

J

Just–In–Time (JIT) industries, costs of downtime to, 93

K

key areas of risk, identifying, 79
key personnel lost/missing, 281–284

L

labor costs/overtime, 92–93
late fees and penalties in, 93
leader selection, for teams, 285–287
legal costs, 93
legal issues of DRP, 14, 15–16
levels of disaster preparedness, 6–8, **7**
libraries
  Save Libraries (SAVLIB) in, 194, **199**
  Virtual Tape Libraries (VTL) in, 200–203, **201**, **203**
library restore, 443–475
  document library, in i5/iSeries restoration, 473
  i5/iSeries restoration, 471–472
  user library, in i5/iSeries restoration, 472
Licensed Internal Code (LIC), 72–73
  Backup Recovery and Media Services (BRMS) and, 478–484, 480*t*, **481**–**484**
  i5/iSeries restoration, 445–450, **447**, **449**, **450**
lifecycle program, backup and, 169–170
likelihood measurement, 79–80
load balancing, 145
locks, 69–71
logs
  backup and, 170
  DSPLOGBRM and, 170
loss of life or missing people, 281–284

M

maintaining the DRP, 42–43, 312–314, 539–561, 587
  change control process and, 544–545, **545**
  change management as part of, 549–560
  company data and, 553–554
  design of plan and, 541–542
  Disaster Recovery Coordinator's role in, 558–559
  distribution technology and, 557–558
  documentation and, 556
  frequency of, 547
  hardware and, 550–551
  importance of, 540–541
  IT recovery team personnel and, 554–555
  "maintenance mode" for, 545–548

need for, 540
philosophy of, implementing, 542–545
reasons for, 547, 547–548*t*
revision tracking in, 560, 560*t*
revisiting the plan for, 545–548
scheduled vs. unscheduled, 548
software and, 551–553
timeframe for, 560–561, **561**
vital record management and, 555
maintenance cost benefits, 226, **226**
“maintenance mode,”, 545–548
map to hotsite, 409–410, **410**, **411**
market trends in disaster recovery, 144–145, **144**
marketing and impact of DR, 4
Maximum Availability, 249
media class, BRMS and, 192
media condition, for tapes, magnetic storage, etc., 73
media coverage, facing and dealing with, 334–337
media identifier, BRMS and, 192
media management, 265–266
media spokesman, 336–337
media, backup, 192
meeting place for command center, selecting, 329–333, **334**
meeting place for recovery team, in event of disaster, 310–314
mirroring, 145, 154–155
missing people and, 281–284
mission statement of DRP, 368–369, **369**
mission-critical servers, 125–127
mission-critical function identification, 96–100, 118–120, **119**
monitoring and maintenance of H/A systems/servers, 241–243
monitoring devices/alarms, 68–69
monitoring risks, 81–82
monthly backups, 193
Murphy’s Law, 12, 81, 85, 534

N

natural disasters, 4, 11–12, 71. *See also* weather related disasters
necessary systems, in server recovery, 125, 134–135, 134–135*t*. *See also* servers
need for disaster recovery plan, 1–47
network recovery team, 300–301. *See also* teams for disaster recovery
network system information for documentation, 440–441
“next off the line” solutions, 151
notification of personnel in disasters, 327–329, 327*t*, 404–405
notification solution design, 338–340

O

objectives of DRP, 20–22, 345, 367–368
objectives of testing, 531–532, **532**, 531
off-site storage, recalling tapes from, 412–413
off-site storage provider, choosing, 271–273. *See also* commercial hotsite providers; hotsites
off-site tape pickup schedule, 267–268, **268**
official privacy notice, 323
open-book testing, 514–515
opening the hotsite, 411–412
operating system restore
Backup Recovery and Media Services (BRMS) and, 492–503, **493**–**502**
i5/iSeries restoration, 459–469, **460**–**467**
operations phase of DRP, 349
opportunity loss, 94–95
optional systems, in server recovery, 124–125. *See also* servers
orphan data, backup of, 172–173
outline of the DRP, 359–365
over-voltage conditions, 56–57

P

partitioning, backup, 235, **235**
passive testing or tabletop exercise, 518–524, 525–528*t*
Personal Information Protection and Electronic Documents Act (PIPEDA), 15
personnel
involved in DRP, 24–26, 89–90. *See also* teams for disaster recovery, 24
loss of, 281–284
notifying of disaster, 404–405
status assessment of, 398

phases of DRP, 17–18, **17**, 341–342, 346–350, **347**
philosophy of maintenance, 542–545
physical security, 69–71
physical threats, 74
planned downtime/maintenance, 102–104, **104**, 147, 220–231, **221**, **223**
- backup and, 199–200, 224–226, **224**, **225**
- dollar value benefit and, 225
- impact of, 102–104, **104**
- maintenance cost benefits for, 226, **226**
- program temporary fix (PTF) installation and, 199–200

planning for disaster recovery (DR), 2–47, 142
planning team for DRP, 24–26, 89–90. *See also* teams for disaster recovery
plumbing leaks. *See* water damage
points of failure, site vulnerability assessment and, 50–51
policies, in BRMS, 192
political threats, 75
power outages, 4, 12. *See also* electrical power supplies
practicing the family DRP, 587
pre-action fire-suppression sprinklers, 68
preparedness, 279–280, 304–305
- levels of, 6–8, **7**
- questions about, 8
- testing the DRP and, 507–508

prevention, 372
prevention phase, DRP, 347–348
primary site restoration team (IT management team), 384
Print System Information (PRTSYSINF) command, 431, 432–434
prioritization of risk, 77–78
prioritizing backups, 187–192, **188–191**
prioritizing recovery systems, 124–125
privacy issues, 15, 16
- contact lists/employee call sheets and, 322–323
- official privacy notice for, 323

productivity losses, 92–93
Program Temporary Fix (PTF), backup and, 199–200
progression of recovery, 384, **385**, **386**, **387**
PRTDSKINF, 173

Q

QINTER, 170
QSYSOPR, 73, 170
questionnaire, Business Impact Analysis (BIA), 117, 591–597

R

Ragged enhancement for SWA saves, 198
RAID disks, 202
reasons for planning, 13–16
reciprocal agreements, 151
recovery, 204–214, 372. *See also* backup
- access path restoration in, 209
- backup lists for Domino and, 213, 213*t*
- BRMS system recovery report and, 207, **208**
- control groups for Domino and, 212, 212*t*
- Critical Control Data (CCD) and, 213–214
- Domino Servers and, tips for, 209–213
- elements in, **206**
- Hardware Management Console (HMC) for, 213–214, **214**
- RESTORE commands and, 204–206, 205*t*
- Restore Object Using BRMS (RSTBRM) in, 212
- system recovery report in, 207, **208**

Recovery Coordinator, 295–296, 297*t*, 307–308, 312–314
Recovery Point Objective (RPO), 32, 36–37, 104–115, **106**, **111**, **113**
- 24-hour, 112–115, **113**
- backup systems and, 129–132, 131*t*, 164
- Business Impact Analysis (BIA) and, 88
- communications and, 318
- high-availability (H/A) servers and, 231
- recovery points defined in, 111–112
- servers and, 129–132, 131*t*
- strategies for recovery and, 141, 143, 146, 147, 159
- vital records management and, 255

recovery progression, 384, **385**, **386**, **387**
recovery script, 417–422
recovery strategies, 34–37
- business impact assessment (BIA) and, 34

Recovery Time Objective (RTO), 31, 36–37, 104–115, **106**, **107**, **108**, 139, 373

backup systems and, 129–132, 131*t*, 164
Business Impact Analysis (BIA) and, 88
communications and, 318
Disaster Recovery Plan (DRP) and, 345
high-availability (H/A) servers and, 231
restoration and, 417
servers and, 125–127, 129–132, 131*t*
strategies for recovery and, 141, 143, 146–147, 159
team for disaster recovery and, 277
vital records management and, 255
Red Cross, 589
regulatory compliance, 14, 15–16, 30, 35, 166
vital records management and, 253
remedial expenses, as cost of downtime, 95
removable media backups and duplication, 203–204
replacement equipment, 304, 414–415
replication, 150
Capacity Backup system from IBM and, 248–250, 249*t*
high-availability (H/A) servers and vs., 234–235
side-by-side systems and, 236–239, **236**
resiliency level of recovery, 156–158, **156**
responsibilities allocation, for DR team, 291–293
restoration, 373, 413–422, 443–475
equipment assessment in, 413–414
i5/iSeries–specific. *See* i5/iSeries restoration
insurance inspection before, 415–416
phases of, 416–417
recovery script in, 417–422
Recovery Time Objectives (RTOs) and, 417
replacing equipment in, 414–415
safety and security established during, 415
sequence of events/timeline in, 418–421, **418**, **422**
RESTORE commands, 204–206, 205*t*
Restore Object Using BRMS (RSTBRM), 212
retention program, vital records, 253–255
Return on Investment (ROI), 36, 88, 105–116, **106**
high-availability (H/A) servers and, 221–231
planned outages and, 147
revenue losses, 91–92
revising the DRP. *See* changes/updates to DRP
revision tracking, 560, 560*t*
risk assessment/analysis, 12, 26–33, **27**, 74–85
Annualized Loss Exposure (ALE) in, 82–84
avoiding risk and, 80
Business Impact Analysis (BIA) vs., 76
cost of downtime and, 79
evaluating risks and, 81–82
example of, 82–84
insurance and, 84–85
issue identification in, 78–79
key area identification in, 79
levels of risk and, 74
measuring likelihood and impact in, 79–80
monitoring risks and, 81–82
physical threats in, 74
political threats in, 75
prioritization of risk in, 77–78
purposes of, 77
risk, frequency, and exposure elements in, 82–84
site vulnerability assessment in, 50–73
solution development and, 80–81
steps/processes in, 77–78, **78**
strategy implementation for, 81
strategy selection for, 81
technological threats in, 74
threat assessment in, 74–75
vulnerability assessment in, 27–28, 49–85
worst case scenarios in, 74
role assignment for DR teams, 289, 291–293
rotating tape media, 251–263
RS232 interface for USP, 60
rules of communication, 331

S

safety, 415
sags in electrical power supplies, 56
sales and impact of DR, 4
Sarbanes-Oxley (SOX) legislation, 15, 166, 253
Save Changed Objects (SAVCHGOBJ), 193–194
Save Libraries (SAVLIB), 194, **199**
Save Option, backup and, 188–192, **188**, **189**
Save Security Data (SAVSECDTA), 194–195, 198–199, **199**
save windows, for backup, 163
save-while-active (SWA) saves, 195–198, **197**, **198**
SAVSECDTA, 430
SAVSTG, 142

SAVSYS, 73
scheduled maintenance, 548
secure transport of vital records, 266
security, 415
  of data, 15, 16
  of hotsite, 568–569
  i5/iSeries restoration, rebuild, 474–475
  Save Security Data (SAVSECDTA) in, 194–195
Security and Exchange Commission (SEC), 15–16
security guards, 69–71
selection criteria for teams, desirable vs. undesirable traits, 277–280, 277*t*
sequence of events/timeline in recovery/restoration, 418–421, **418**, **422**
serious injury, 282
servers, 33–40, 123–137, 139
  A-list recovery strategy for, 124, 132–134, 133*t*, 380, 380*t*
  alternate installation devices for, 71–72
  B-list recovery strategy in, 125, 134–135, 134–135*t*, 381, 381*t*
  backup partitioning and, 235, **235**
  backup priorities for, ranking, 127–129, 129*t*
  backup strategies for, 37–38
  Business Impact Analysis (BIA) and, 124
  clustering of, 35
  commitment control, transaction processing and, 35
  continuous systems availability and, 234–235
  cost of downtime and, 131–132
  critical systems in, 124–125, 132–134, 133*t*
  criticality assessment of, 33–40, 123–137
  Domino. *See* Domino Servers
  email and, as mission-critical application, 135
  essential systems in, 124–125
  hardware requirements for mission-critical, 135–136
  high-availability techniques for, 35, 36, 39–40, 143
  hotsites and, 35
  license internal code CD and, 72–73
  loss of, vs. server, 434–441
  maintenance cost benefits for, 226, **226**
  mission-critical systems in, 125–127
  monitoring and maintenance for, 241–243
  necessary systems in, 125, 134–135, 134–135*t*
  optional systems in, 124–125
  prioritizing recovery of systems in, 124–125
  ranking criticality of, 123–137
  Recovery Point Objectives (RPO) and, 129–132, 131*t*
  recovery strategies for, 34–37
  Recovery Time Objectives (RTO) and, 125–127, 129–132, 131*t*
  regulatory compliance and, 35
  replication in, 234–235
  restoration process definition and documentation for, 352
  size of, in H/A systems, 239–241, **240**
  system priority in, classifying for recovery, 124–125
  tape-based recovery for, 35
  target/source compatibility in, 243–244
  workload balancing in, cost benefit of, 227–230, **227**, **228**
Service Level Agreement (SLA), 40
shadowing, 145
shift work schedules, for DR teams, 306
shock, physiologic, 9
shock hazards, electrical, 55
side-by-side systems, 236–239, **236**
site vulnerability assessment, 50–73
  alternate installation devices and, 71–72
  electrical power supplies in, 55–62
  facility monitoring devices/alarms in, 68–69
  fire suppression systems in, 65–68
  humidity levels in, 52–54
  license internal code CD and, 72–73
  media condition in, 73
  natural disaster safeguards in, 71
  physical security in, 69–71
  points of failure in, 50–51
  smoke detection for, 63, 66
  temperature levels in, 52–54
  water detection for, 62–65
size of H/A servers, 239–241, **240**
smoke detectors, 63, 66
software
  disaster recovery plan (DRP) and, 376–378, **379**

maintenance and change management in, 551–553
spikes, 56
sprinkler systems, 65–68. *See also* fire-suppression systems
staff commitment to DRP, 22–24
staffing of command center, 330
Start Backup Using BRMS (STRBKUBRM), 210
static electricity, 55
steps of risk management, 77–78, **78**
storage time for tapes, 264, **264**
strategies for recovery, 139–159, **146**
alternate sites in, 154
backup, 148–150
checklist for, 157, 158*t*
cold sites in, 152–153
comprehensive nature of, 143
cost of, 143–144, 147
data center solutions for, 150–155
definition of, 140–141
determining resiliency level for, 156–158, **156**
drop ship solutions in, 152
flexibility of, 142
flowchart/sample of, 158, **159**
goals of, 141, 143
high availability (HA) and, 143, 145
hotsites in, 153–154
information required for, 139
load balancing and, 145
market trends in, 144–145, **144**
mirroring and, 145, 154–155
“next off the line” in, 151
planned outages and ROI in, 147
planning for, 142
reciprocal agreements in, 151
Recovery Point Objectives (RPO) in, 141, 143, 146, 147, 159
Recovery Time Objectives (RTO) in, 141, 143, 146–147, 159
replication in, 150
requirements of, 139–159
selection guidelines for, 141–144
shadowing and, 145
tape backups and, 145, 147–148
warm/hot sites in, 145
stress management, 283–284
structural attributes of DRP, 345–346
structure/outline of the DRP, 359–365
style of the DRP plan, in writing, 357–358
supported services in DRP, 375–376
surges and surge suppression, 55, 56
system recovery report, BRMS, 207, **208**
system security rebuild, i5/iSeries restoration, 474–475
systems documentation. *See* documentation, system-related
systems priority in recovery, 124–125

T

table of contents of DRP, 366
tabletop exercise, 518–524, 525–528*t*
tangible cost analysis, 90–93, **91**
tape backup, 72–72, 145, 147–148, 162
alternate installation devices for, 71–72
alternate sites in, 154
authorization list for, 412–413, **413**
Backup and Recovery Media Services and BRMS command for, 181, 260
cold sites in, 152–153
condition of tapes for, 259–260
documentation vs., 429–431
drive maintenance for, 260–261
drop ship solutions in, 152
duplicate volumes in, 184
error monitoring in, 182–184, **183**
expiration dates in, 180–181
expiry dates for, 261
grandfather, father, son (GFS) strategy for, 262–263, **263**
hotsites form, 153–154
Initialize Tape (INZTAP) command and, 177–180, **180**, 182, 259
labeling tapes for, 260
maintaining drives for, 181
media condition in, 73
mirroring in, 154–155
naming and labeling of, 177
“next off the line” strategy and, 151

tape backup, 72–72, 145, 147–148, 162
- off-site tape pickup schedule for, 267–268, **268**
- preparing, 177–180
- pros and cons of, 166
- protecting tapes from corruption in, 171–172, **171**
- recalling tapes from off-site storage provider in, 412–413
- reciprocal agreements in, 151
- retention of backup tapes used in, 176–177
- rotating off-site tapes for, 251–263
- storage of tapes in, 182
- storage time for tapes containing, 264, **264**
- tape media management policies for, 265–266
- timeline to rebuild, 108–109, 109*t*
- Virtual Tape Libraries (VTL) in, 200–203, **201**, **203**
- vital records management and, 259–260

tape-based recovery, 35

tape media management policies, 265–266

target/source compatibility, in H/A systems, 243–244

tasks assignment, for disaster recovery teams, 291–293

teams for DR, 24–26, 275–315, 327–373, 381–388, **382**, 392–393
- administrative responsibilities in, 305
- alert notification procedure for, 393–396
- application recovery team in, 302
- assembly of, at command center, 399–400
- building of, 284–289
- call sheet for, who to contact in event of emergency, 323–329, **324**
- caring for, during disaster, 305–310
- chain of command established for, 297–298
- command-center stress and, 283–284
- communication between leaders and members of, 287–288
- death or serious injury in, 282
- disaster recovery plan (DRP) and, 381–388, **382**
- DR testing and plan maintenance by, 312–314
- effect of disaster on people and, 280
- established organization of, understanding, 350–351
- facility recovery team in, 303
- food supplies for, 306–307
- goal setting for, 289
- hardware recovery team in, 301–302
- importance of, 275–277
- IT recovery management team in, 293–298, 371, 382–383, 383*t*
- IT recovery team personnel and, 554–555
- IT technical recovery team in, 298–300, 383–384, 384*t*
- leader selection for, 285–287
- loss of life or missing people and, 281–284
- meeting of, in event of disaster, 311–312
- meeting place for, in event of disaster, 310–314
- network recovery team in, 300–301
- overview of, 290–291
- preparation of, 279–280
- preparedness of, 304–305
- primary site restoration team (IT management team) in, 384
- Recovery Coordinator and, 295–296, 297*t*, 307–308, 312–314
- Recovery Time Objectives (RTOs) and, 277
- reducing numbers of, for testing, 524–525
- replacement equipment for, 304
- responsibilities allocated among, 291–293
- role assignment in, 289, 291–293
- selection criteria for, desirable vs. undesirable traits, 277–280, 277*t*
- shift work schedules for, 306
- tasks assignment in, 291–293
- Technical Recovery Manager in, 299, 300, 312–314
- test teams and, 517–518
- travel guidelines for, 309, **310**
- working together as, 289–293

Technical Recovery Manager, 299, 300, 312–314

technological risks, 30

technological threats, 74

technology recovery from backup 164–165

technology requirements for DRP, 37

telephone service notification, 1-800 services, 339

temperature levels
- fire-suppression systems and, 65–66
- portable cooling units and, 54–55

site vulnerability assessment and, 52–54
UPS and, cooling the UPS room, 58–59
tendering an offer for hotsite services, 574–576
testing call-notification process, 318, **318**
testing H/A systems, 245–248
testing hotsite access, 573
testing the DRP, 44–46, 312–314, 352–353, 373, 507–538
active, 529–532
benefits of, 536–538
consistency of plan and, 515
defining a complete project for, 515–518
Disaster Recovery Coordinator's role in, 533–534
evaluating results of, 535–536
failure shown by, 512–514
frequency of, 510, 536
goals of, 512
importance of, 508–509
Murphy's Law and, 534
need for, 511–512
objectives and goals for, 531–532, **532**
open-book, 514–515
passive or tabletop exercise, 518–524, 525–528*t*
preparedness and, 507–508
reducing the team for, 524–525
responsibilities during, 514
staffing required for, 517–518
Three-Step Special, 529–531
types of, 516
threat assessment, 74–75
Three-Step Special testing, 529–531
time to recovery. *See* recovery time objective (RTO)
timeframe for maintenance, 560–561, **561**
timeline in recovery/restoration, 418–421, **418**, **422**
title page of DRP, 365–366
tools to aid in DRP writing, 357–358
tornadoes, 12, 71
touring hotsite facilities, 569–570
transaction processing, commitment control and, 35
travel guidelines, team for disaster recovery and, 309, **310**
types of disasters, 11–12

U

under-voltage conditions, 56–57
uninterruptible power supplies (UPS), 56–62, 81, 568
battery replacement in, 57
disposal of batteries in, 58
air conditioning for, 58–59
RS232 interface for, 60
highly redundant power supply configuration and, **60**, 61–62
diesel and natural-gas generator backups for, 61–62
unscheduled maintenance/downtime, 548
updating the DRP. *See* changes/updates to DRP
user library restore, in i5/iSeries restoration, 472
user profile restore, in i5/iSeries restoration, 469–470, **470**

V

validating the DRP, 43–46, **43**, 352–353
vendor information for hotsite, 406
verification of restore, in i5/iSeries restoration, 473–474
Virtual Tape Libraries (VTL), 200–203, **201**, **203**
Vision Solutions, 249
vital records management, 251–273
barcode support for, 266
Business Impact Analysis (BIA) and, 252
container identification tag for, **271**
container vaulting for, 266
defining vital records for, 252, 253
environmental controls for, 267
expiry dates for, 261
family documents as, 587
grandfather, father, son (GFS) strategy for, 262–263, **263**
individual media vaulting for, 267
maintaining the DRP and, 555
media management in, 265–266, 265
off-site storage considerations for, 268–271, **258**
off-site storage provider for, choosing, 271–273
off-site tape pickup schedule for, 267–268, **268**
on-site storage of, vs. off-site, 255–259
on-site vulnerability assessment for, 266

vital records management, *continued*
  Recovery Point Objectives (RPOs) for, 255
  Recovery Time Objectives (RTOs) for, 255
  regulatory compliance and, 253
  retention program for, 253–255
  rotating off-site tapes for, 251–263
  secure transport of, 266
  storage time for tapes containing, 264, **264**
  tape condition for, 259–260
  tape drive maintenance for, 260–261
  tape media management policies for, 265–266
vulnerability assessment, 27–28, 48–85. *See also* risk assessment
  physical security in, 69–71
  site vulnerability assessment, 50–73
  vital records management and, 266

W

warm sites, 145
water damage, 12, 62–65
water detection systems, 62–65
water supplies, 586
weather-related disasters, 4, 11–12, 71. *See also* natural disasters
web site notification in regional disasters, 338
weekly backups, 193
wet-pipe fire suppression/sprinkler systems, 67
who to contact in event of emergency, 323–329, **324**
windows, 69–71
workload balancing, cost benefit of, 227–230, **227**, **228**
workshop approach to mission-critical function identification, 97–99
worst-case scenarios, 74
writing the DRP, 353–359