

Index

Boldface text indicates tables or illustrations.

A

- Access Client Solutions (ACS), 10, 175, 250–251
- Access control, 3, 7, 8, 380
 - application security and, 286–287
 - application-only access in, 291
 - classification of data and, 16, 18
 - Internet security and, 273–274
 - menu access control in, 287–290, **288**
 - object-level security and, 358
 - role-based, 104, 303–321. *See also* Role-based access
- ACCTNG profile, 355
- Active Directory (AD), 23
 - networks and connectivity in, 239
 - user profiles and, 90
- ADD, 379
- Add Community for SNMP (ADDCOMSNMP), 247
- Add Server Authentication Entry (ADDSVRAUTE), 248–249, 250
- ADD, **148**, 150–151, **152**, **197**
- ADDCOMSNMP, 247
- ADDSVRAUTE, 248–249, 250
- Administration. *See* Security administration
- Adopted authorities, 56–57, 166–170, **167**, 362–363
 - integrated file system (IFS) and, 201–202, 205
- AES, 225
- Algorithms, encryption. *See* Encryption
- ALL, 156, 172–174
- ALLOBJ, 3, 9, 28, **29**, **30**, **98**, 99, 380
 - adopted authority and, 166–170, **167**
 - application security and, 289–290
 - auditing and, 323
 - authority checking for, 163–166, **163**
 - compliance issues and, 385
 - encryption and, 231
 - object-level security and, 147
 - ownership of objects and, 172–174
 - resource security and, 29
 - role-based access and, 317–318, 317
 - row/column access control (RCAC) and, 180, 181, 184–185
 - security level 30 and, 30
- Allow Object Differences (ALWOBJDIF), 33
- Analyze Default Password (ANZDFTPWD), 93, 110, 272, 386
- Analyze Profile Activity (ANZPRFACT), 110
- Annual security assessments, 388–389
- Anonymous FTP, 243
- ANZDFTPWD, 93, 110, 272, 386
- ANZPRFACT (Analyze Profile Activity), 110

- Application Administration, 174–179, **176**, **177**, **178**, 252
- Application programming interfaces (APIs)
 - profile-swap and profile-token, 292
 - security level 40 and, 31
- Application security, 20, 283–301
 - ALLOBJ in, 289–290
 - application-only access in, 291
 - audit trails and, 295–296
 - authorities for, 296
 - authorization schemes for, 287–293
 - changes to apps and, 368–371
 - changing the process in, 292
 - connectivity and, 298
 - Dedicated System Tools (DSTs) and, 297
 - design considerations in, 285–296
 - encryption and, 298
 - exit points/programs in, 297–289
 - group authority in, 289
 - implementation details in, 296–300
 - job descriptions and, 299
 - library lists and, 299
 - library-qualified calls and, 299–300
 - logging and, 294
 - menu access control in, 287–290, **288**
 - object-level security and, 368–371
 - ownership of application in, 293
 - passwords and, 297, 300
 - profile-swap APIs and, 292
 - profile-token APIs and, 292
 - PUBLIC authority in, 289, 296, 298, 299
 - QSECOFR and, 296, 297
 - risk assessment for, 284–285
 - roles and access control in, 286–287
 - security levels for, 298
 - System Service Tools (SSTs) and, 297
 - system values and, 297
 - testing, 300–301
 - UID and GID APIs and, 292–293
 - user profiles and, 292–295, 297
 - vendors and, 297
- Application-only access, 291
- Appropriate use of data, 16–17
- Architecture, object-level security, 355–356
- Asymmetric keys, 224–226, **225**
- ATNEVT, **330**
- Attributes, file, in IFS, 200–201, **201**
- Audit journal, 328, 340–349. *See also* Auditing
- AUDIT, **29**, **30**, **98**
- Auditing, 323–352
 - ALLOBJ and, 323
 - application security and, 295–296
 - audit journal in, 328, 340–349
 - auditing control security recommendations in, 339
 - AUDLVL (User Action Auditing) in, 330–333, **330–331**, 334, 339
 - AUTFAIL in, 332, 339
 - benefits of, non-security related, 324
 - Change Auditing Value (CHGAUD) in, 336
 - Change Object Auditing (CHGOBJAUD) in, 335–338, **335**, **336**
 - Change Security Auditing (CHGSECAUD) in, 328, **329**, 350
 - Change User Audit (CHGUSRAUD) in, 317, 334–335, **334**, 340
 - compliance issues and, 323
 - controls for, 329
 - Copy Audit Journal Entries (CPYAUDJRNE) in, 143, 187, 347, **348**, 351
 - CREATE in, 332
 - Create Journal Receiver (CRTJRNRCV) in, 328
 - Create User Profile (CRTUSRPRF) in, 334
 - CREATE, 339
 - DELETE in, 332, 339
 - determining whether auditing should occur, 337, **337**
 - Display Audit Journal Entry (DSPAUDJRNE) in, 343–344, **344**, **345**, 350

- Display Journal (DSPJRN) in, 345–347, **346**
- Display Log (DSPLOG) in, 325–327, **325**, **326**
- Display Security Auditing (DSPSECAUD) in, 351
- displaying/printing audit journal entries in, 343–347
- end session in, QAUDENDACN, 77
- events and, recommendations for, 338–340
- Financial Instruments and Exchange Law (JSOX) and, 323
- force level for, QAUDFRCLVL, 78, 329
- formats for journal entries, 340–341, **341–343**
- High Availability (HA) systems and, 324
- history log in, 325–327
- IBM i architecture and, benefits of, 350
- incident response and, 396–397, 398
- integrated file system (IFS) and, 202
- JOBBAS in, 333
- JOBDTA in, 333
- level of, extending, QAUDLVL2, 82
- level of, QAUDLVL, 78–82
- Navigator for i and, 351–352, **351**
- new object, QCRTOBJAUD, 83–84, 338
- OBJAUD (Object Auditing) in, 335–338, 339
- object auditing in, 335–338, 339
- object-level security and, 358–360
- PGMADP in, 333
- proactive stance to, 324
- PRTDTA in, 333
- PTFOPR in, 332, 339
- QAUDCTL (Auditing Control) in, 329, 339
- QAUDENDACN in, 339
- QAUDFRCLVL (Auditing Force Level) in, 329, 339
- QAUDLVL (Auditing Level) in, 317, 329–333, **330–331**, 339, 340, 341
- QAUDLVL2 (Auditing Level Extension) in, 329–333, **330–331**
- QAUJRN in, 341
- QCRTAUT (Create Authority) and, 338
- QCRTOBJAUD (Auditing for New Objects) in, 338
- QHSTLOGSIZ (History Log Size) in, 326
- QSECOFR in, 332, 333
- reporting on activities from audit journal in, 348–349
- Sarbanes-Oxley Act (SOX) and, 323
- saving journals, timing for, 398
- SAVRST in, 332, 339
- SECCFG in, 333, 339
- SECRUN in, 333, 339
- security audit journal in, 327
- SECURITY in, 333
- SERVICE in, 333, 339
- service tools and, 143
- SPLFDTA in, 333
- system security and, 339
- system values for, 75–84, **76**, 329–333, **330–331**
- system-wide, 329–333
- tools for, 350
- user auditing and, 334–335, **334**
- AUDLVL (User Action Auditing) in 330–333, **330–331**, 334, 339
- AUT (Authority), 108–109, 156, 218
- AUTCHK (Authority Check) parameter, 217–218
- AUTFAIL, **330**, 331, 332, 339
- Authentication
 - Add Server Authentication Entry (ADDSVRAUTE) in, 248–249, 250
- Authorities, 148–153, 379
 - ADD in, 150–151
 - adopted, 166–170, **167**, 201–202, 205, 362–363
 - application security and, 289
 - AUT (Authority) in, 108–109
 - AUTCHK (Authority Check) parameter in, 217–218
 - authority cache and, 166

- authority checking in, 162–166, **163**, **165**
- authorization lists and, 160–162, **160**, 364–365, 364
- categories of, **148**
- Change Authority (CHGAUT) in, 198–200, **200**
- collection of, authority collection, 189–193
- compliance issues and, 387, 390
- Create Authority (CRTAUT) in, 43–44, 156–160
- data, 148, 150–151
- default PUBLIC, 158–160
- Display Authority (DSPAUT) in, 198, 387
- Display Object Authority (DSPOBJAUT) in, 155, 186, 379, 387
- DLT in, 151–152
- Edit Authorization List (EDTAUTL) in, 160
- Edit Object Authority (EDTOBJAUT) in, 148, 155, 161, 186
- EXCLUDE and, 151, 152, 153, 158–160, 163
- Grant Object Authority (GRTOBJAUT) in, 148, 153, 160, 161
- group profiles and, 153–155, 289
- groupings of, 152–153
- GRPAUT (Group Authority) in, 104–107
- GRPAUTTYP (Group Authority Type) in, 104–107, 154
- integrated file system (IFS) and, 196–202, **197**, 209–210
- IOSYSCFG special authority and, 236
- limited user function (application administration) and, 174–179, **176**, **177**, **178**
- Navigator for i and, 193–194, **194**
- networks and connectivity in, 236
- OBJALTER in, 150
- object, 148, 149–150, 362
- OBJEXIST in, 149–150
- OBJMGT in, 149–150
- OBJOPR in, 149–150
- OBJREF in, 150
- ownership of objects and, 172–174
- Print Adopting Objects (PRTADPOBJ) in, 193
- Print Private Authorities (PRTPVTAUT) in, 193, 213, 387
- Print Public Authorities (PRTPUBAUT) in, 193, 213, 387
- Print Queue Authority Report (PRTQAUT) in, 222
- printers, printed output, and, 218–219, **219**
- private authorities by IBM in, 205
- private, 109, 148–153
- PUBLIC, 155–160, 163–165, 289, 364, 365, 366–367
- QCRTAUT (Create Authority) and, 156–160, 338
- QPWFSEVER authorization list and, 211
- R (Read) authority in, 196
- READ in, 150–151
- relationships among, 151–152
- Restore Authority (RSTAUT) in, 154, 398, 399
- Revoke Object Authority (RVKOBJAUT) in, 148, 161
- root directory and, 209
- row/column access control (RCAC) and, 183–184
- RX data authority and, 205
- Save/Restore functions and, 170–172
- SECBATCH tools for, 193, **193**
- SECTOOLS tools for, 193, **193**
- SPCAUT (Special Authority) in, 97–101
- SPLCTL special authority in, 218
- Start Authority Collection (STRAUTCOL) in, 189–190, **190**
- system values for, 43–44, 56–57
- tools for, 193
- UPD in, 150–151
- Use Adopted Authority (USEADPAUT), 168
- user profiles and, 109
- viewing a user’s capabilities in, 177, **177**

- W (Write) authority in, 197
- Work with Authority (WRKAUT) and, 198–200, **199**
- X (Execute) authority in, 197
- Authority cache, 166
- Authorization lists, 160–162, **160**, 364–365
 - compliance issues and, 390–391
 - Display Authorization List (DSPAUTL) in, 387, 390
 - Display Authorization List Objects (DSPAUTLOBJ) in, 387, 390
 - QPWFSEVER and IFS in, 211
- Authorization schemes, 287–293
- AUTLMGT, **148, 197**
- AUTOSTART, networks and connectivity, 239
- Auxiliary storage pools (ASPs), encryption, 233
- Availability of data, 5
- Awareness. *See* Security awareness program

- B**
- Backup and recovery, 371–373. *See also* Incident recovery plan
- Backup Recovery and Media Services (BRMS), 175
 - encryption and, 232–233
- Blogs, 22
- BOSS option 47, in RCAC, 179
- Bring Your Own Device (BYOD) issues, 20–21
- Business contingency plans, 282

- C**
- Cache, authority, 166
- Calls, library-qualified, 299–300
- Case-sensitive passwords, 130, 131
- Certificate Authorities (CA), 257, 258–261
- CFGTCP, 240
- CHANGE, 156
- Change Activation Schedule Entry (CHGACTSCDE), 110
- Change Active Profiles List (CHGACTPRFL), 110
- Change Auditing Value (CHGAUD), 336
- Change Authority (CHGAUT), 198–200, **200**
- Change Command Default (CHGCMDDFLT), 239
- Change DDM TCP/IP Attributes (CHGDDMTCPA), 248
- Change Expiration Schedule Entry (CHGEXPSCDE), 110
- Change FTP Attribute (CHGFTPA), 239
- Change Function Usage (CHGFCNUSG), 178, 252
- Change Job Description (CHGJOBDD), 32
- Change Library (CHGLIB), 43–44
- Change Object Auditing (CHGOBJAUD), 335–338, **335, 336**
- Change Object Owner (CHGOBJOWN), 172–174
- Change Object Primary Group (CHGOBJPGP), 155
- Change Output Queue (CHGOUTQ), 216
- Change Password (CHGPWD), 60, 378
- Change Password (QSYSCHGPW), 60, 95
- Change Security Auditing (CHGSECAUD), 328, **329, 350**
- Change Service Tools User Privileges, 133–136, **133, 134**
- Change System Value (CHGSYSVAL), 28
- Change User Audit (CHUSRAUD), 317, 334–335, **334, 340**
- Change User Profile (CHGPRF), 102
- Change User Profile (CHGUSRPRF), 52, 87, 168, 292
- CHGACTPRFL, 110
- CHGACTSCDE, 110
- CHGAUD, 336

- CHGAUT, 198–200, **200**
- CHGCMDDFT, 239
- CHGDDMTCPA, 248
- CHGEXPSCDE, 110
- CHGFCNUSG, 178, 252
- CHGFTP, 239
- CHGJOB, 32
- CHGLIB, 43–44
- CHGOBJAUD, 335–338, **335**, **336**
- CHGOBJOWN, 172–174
- CHGOBJPGP, 155
- CHGOUTQ, 216
- CHGPRF, 102
- CHGPWD, 60, 378
- CHGSECAUD, 328, **329**, 350
- CHGSYSVAL, 28, 84
- CHGUSRAUD, 317, 340
- CHGUSRPRF, 52, 87, 168, 292
- Chief Security Officer (CSO), 401
- CHUSRAUD, 334–335, **334**
- CIPHER, 226
- Cipher management, system values, 59
- Classification of data, 15–19
 - access control and, 16, 18
 - appropriate use of data and, 16–17
 - confidential data in, 17
 - confidential until announced data in, 17
 - deny by default concept in, 16
 - disposal of data and, 16, 18
 - encryption and, 16, 18
 - IT department and, 18–19
 - ownership of data and, 18
 - private data in, 17
 - public data in, 17
 - responsibility for, 17–18
 - restricted data in, 17
 - retention of data and, 16, 18
 - security measures and, 16
 - systems for, 17
- Client Access, 10
- Cloud computing, Internet security, 278–281
- CMD, **330**
- Column masks, 185–186
- Common Criteria for Information Tech Security Evaluation, 27, 41
- Communicating importance of security, 402–403
- Communications security, 256–262. *See also*
 - Networks and connectivity, 256
 - Certificate Authorities (CA) in, 257, 258–261
 - Digital Certificate Manager (DCM) in, 258, 261
 - digital certificates in, 257, 258
 - HTTPS in, 258, 259
 - QSSLCSL and, **260**
 - QSSLCSLCTL and, **259**
 - QSSLPCL and **260**
 - Secure Shell (SSH) in, 262
 - virtual private networks (VPNs) and, 261
- Community names, in SNMP, 247
- Compliance, 9, 383–392. *See also* Incident response plan
 - annual security assessment and, 388–389
 - auditing and, 323
 - authorization lists and, 390–391
 - evaluating key areas for, 384–387
 - group profiles and, 390
 - object authority and, 387
 - object-level security and, 373
 - policies and processes for, 391–392
 - reviewing security and, 389–391
 - role-based access and, 303
 - security policies and, 22–23
 - special authorities and, 390
 - system values and, 385
 - user profiles in, 385
- Confidential data, 4, 17
- Configuration, system values, 42

Configure TCP/IP (CFGTCP), 240
 Connectivity. *See* Networks and connectivity
 Consultants, role-based access, 319–321
 Contingency plans, 282
 Control-block modification, 35
 Copy Audit Journal Entries (CPYAUDJRNE),
 143, 187, 347, 3481, 351
 Copy Spooled File (CPYSPLF), 216, 219
 Copy to Import File (CPYTOIMPF), 207
 Copy to Stream File (CPYTOSTMF), 207
 CPYAUDJRNE, 143, 187, 347, 3481, 351
 CPYSPLF, 216, 219
 CPYTOIMPF, 207
 CPYTOSTMF, 207
 CREATE, 331, 332, 339
 Create Authority (CRTAUT), 43–44, 156–160
 Create CL Program (CRTCLPGM), 169
 Create Directory (CRTDIR), 380
 Create Job Description (CRTJOB), 32
 Create Journal Receiver (CRTJRRCV), 328
 Create Library (CRTLIB), 43–44, 380
 Create Output Queue (CRTOUTQ), 216–218,
 220–222
 Create Service Tools User ID, **129**
 Create User Profile (CRTUSRPRF), 87–89, 105,
 192, 334
 CREATE, **330**
 CRTAUT, 43–44, 156–160
 CRTCLPGM, 169
 CRTDIR, 380
 CRTJOB, 32
 CRTJRRCV, 328
 CRTLIB, 43–44, 380
 CRTOUTQ, 216–218, 220–222
 CRTUSRPRF, 87–89, 105, 192, 334
 Current Library (CURLIB), 101

D

DASD, 175
 Data areas, 150
 Data authorities, 148, 150–151
 Data Encryption Standard (DES), 129
 Data preservation, incident response, 396
 Data queues, 150
 Data transfer issues, 251
 DDM. *See* Distributed Data Management
 DDMACC (DDM Access) attribute, 237, 238
 Debugging, 371–373, 371
 Dedicated Service Tools (DST), 127, 137, 297
 Defamation, 22
 DELETE, **330**, 331, 332, 339, 379
 Delete User Profile (DLTUSRPRF), 87
 Deny by default concept, 16
 Design considerations
 application security and, 285–296
 object-level security and, 355
 Device management, 250–255
 Access Client Solutions (ACS) and, 250–251
 data transfer issues in, 251
 device profiles in, 139–141
 mobile devices in, 250–255
 PCs, 250–255
 PCSACC (PC Support Access) attribute for,
 237, 238
 QAUTOCFG (Automatic Device
 Configuration) system value in, 236
 QAUTOVRT (Automatic Config of Virtual
 Devices) system value in, 236
 remote command issues in, 251
 Device profiles, 139–141
 Device sessions, 49–50
 Digital Certificate Manager (DCM), 258, 261
 Digital certificates, 257, 258
 Digital signatures, 58

- Disaster recovery considerations, encryption and keys, 233–234
 - Disconnect intervals, system values, 47–49
 - Display Activation Schedule (DSPACTSCD), 110
 - Display Active Profiles List (DSPACTPRFL), 110
 - Display Audit Journal Entry (DSPAUDJRNE), 343–344, **344**, **345**, 350
 - Display Authority (DSPAUT), 198, 387
 - Display Authorization List (DSPAUTL), 387, 390
 - Display Authorization List Objects (DSPAUTOBJ), 387, 390
 - Display Authorized Users (DSPAUTUSR), 386
 - Display Expiration Schedule (DSPEXPSCD), 110
 - Display Function Usage (DSPFCNUSG), 178, 252
 - Display Journal (DSPJRN), 345–347, **346**
 - Display Log (DSPLOG), 325–327, **325**, **326**
 - Display Object Authority (DSPOBJAUT), 155, 186, 379, 387
 - Display Security Auditing (DSPSECAUD), 351
 - Display Service Tools User ID, 138, **139**
 - Display Spooled File (DSPSPLF), 219
 - Display Station Passthrough (DSPT), 42
 - Display System Value (DSPSYSVAL), 28, 385
 - Display User Profile (DSPUSRPRF), 192, 378, 386
 - Disposal of data, 16, 18
 - Distributed Data Management (DDM), 7, 8, 181, 290
 - DDMACC (DDM Access) attribute for, 237, 238
 - integrated file system (IFS) and, 211
 - networks and connectivity in, 247–250
 - Distributed Relational Database Architecture (DRDA), 238
 - networks and connectivity in, 247–250
 - DLT, **148**, 151–152, **152**, **197**
 - DLTUSRPRF, 87
 - Document Library Objects (DLOs), 190, **196**
 - Documentation of security, 10
 - Domain Name Service (DNS), 246
 - Domain restrictions, 31–32
 - Downloads, Internet security, 267
 - DSPACTPRFL, 110
 - DSPACTSCD, 110
 - DSPAUDJRNE, 343–344, **344**, **345**, 350
 - DSPAUT, 198, 387
 - DSPAUTL, 387, 390
 - DSPAUTOBJ, 387, 390
 - DSPAUTUSR, 386
 - DSPDTA (Display Data) parameter, 216–217
 - DSPEXPSCD, 110
 - DSPFCNUSG, 178, 252
 - DSPGNINF, 104
 - DSPJRN, 345–347, **346**
 - DSPLOG, 325–327, **325**, **326**
 - DSPOBJAUT, 155, 186, 379, 387
 - DSPSECAUD, 351
 - DSPSPLF, 219
 - DSPSYSVAL, 28, 385
 - DSPUSRPRF, 192, 378, 386
 - DTAARA, 150
 - DTAQ, 150
 - Dynamic SQL
 - object-level security and, 361
 - user profiles and, 170
- E**
- Edit Authorization List (EDTAUTL), 160
 - Edit Object Authority (EDTOBJAUT), 148, 155, 161, 186
 - EDTAUTL, 160

- EDTOBJAUT, 148, 155, 161, 186
- Elliptic Curve, 225
- Email, 22
- Post Office Protocol (POP) in, 245–246
 - Simple Mail Transfer Protocol (SMTP) in, 244–245
 - Work with Names for SMTP (WRKNAMSMTP) in, 245
- Employee guidelines, 21–22
- Encryption, 16, 18, 223–234
- access to keys and routines in, 231
 - AES, 225
 - algorithms for, 223, 224
 - ALLOBJ and, 231
 - APIs supplied by IBM for, 226–232
 - application architectures and choice of, 229–230
 - application security and, 298
 - areas for, 223
 - asymmetric keys in, 224–226, **225**
 - auxiliary storage pools (ASPs) and, 233
 - backing up keys for, 231
 - backup media and, 232–233
 - changing keys for, 231–232
 - CIPHER and, 226
 - classification of data and, 16, 18
 - Data Encryption Standard (DES), 129
 - determining data requiring, 227–229
 - disaster recovery considerations and, 233–234
 - Elliptic Curve, 225
 - Federal Information Processing Standards (FIPS) and, 226–227
 - key management policies for, 230
 - key storage in, 230–231
 - keys for, 223, 224
 - networks and connectivity in, 257–262
 - Payment Card Industry Data Security Standard (PCI DSS), 226
 - planning for, 234
 - process of, 226–232
 - public key infrastructure (PKI) in, 224–226, **225**
 - public/private key pairs in, 225
 - RC5, 225
 - resources for, 234
 - RSA in, 225
 - scope of, 227–229
 - Secure Hash Algorithm (SHA) in, 130
 - separation of duties in management of, 230
 - symmetric keys in, 224–226, **225**
 - transmission of data and, 226
 - Transport Layer Security (TLS) and, 225, 257–262
 - Triple DES, 225
 - virtual private networks (VPNs) and, 226
- End Host Server (ENDHOSTSVR), 252
- End TCP/IP (ENDTCP), 252
- ENDHOSTSVR, 252
- ENDTCP, 252
- Enforcement of security policies, 22–23
- Enterprise Identity Mapping (EIM), 249
- EXCLUDE, 108–109, **148**, 153, 156, 158–160, 163, 379, 380
- integrated file system (IFS) and, 208–209
- EXECUTE, **148**, 151, 152, **152**, **197**, 379
- Exit points/programs, 276–277
- application security and, 297–289
- Expiration warning for passwords, QPWDEXPWRN, 71, 75
- Extranets, 19–20
- F**
- Federal Information Processing Standards (FIPS), 226–227
- File attributes, 200–201, **201**
- File ID (FID), 202
- File shares, 202–205, **203**, **204**, 211–212
- File system management, system values, 55–56.
- See also* Integrated file system (IFS)

File Transfer Protocol (FTP), 7, 8, 181, 241, 242–244, **243**, 257, 290

Change FTP Attribute (CHGFTP) in, 239
integrated file system (IFS) and, 202, 211
user profiles and, 85

Financial Instruments and Exchange Law (JSOX), 323

Firewalls, 267, 268–270, **269**

Force conversion, 45–47

Force level, auditing, QAUDFRCLVL, 78, 329

Functional privileges, 128

Functions

Change Function Usage (CHGFCNUSG) in, 178, 252

defining a secure environment for, 311

Display Function Usage (DSPFCNUSG) in, 178, 252

User Function Registration APIs in, 175

Work with Function Usage (WRKFCNUSG) in, 178, 252

G

General system values, 38–60

Gramm-Leach-Bliley Act (GLBA), 303

Grant Object Authority (GRTOBJAUT), 148, 153, 160, 161

Group authority, 289. *See also* Group profiles

Group Identification Number (GID), 108

Group IDs, 292–293

Group Policy Objects (GPOs), 252–253

Group profiles, 104–109, 153–155, 379. *See also*
Role-based access

assigning, to a user profile, 106–107

authority checking and, 165–166, **165**

compliance issues and, 390

Create User Profile (CRTUSRPRF) in, 105

Group Identification Number (GID) in, 108

GRPAUT (Group Authority) in, 104–107

GRPAUTTYP (Group Authority Type) in, 104–107, 154

GRPPRF (Group Profile) in, 104–107, 153–154

OWNER in, 104–107

role-based access and, 104, 305–308

SUPGRPPRF (Supplemental Groups) in, 104, 154

GRPAUT (Group Authority), 104–107

GRPAUTTYP (Group Authority Type), 104–107, 154

GRPPRF (Group Profile), 104–107, 153–154

GRTOBJAUT, 148, 153, 160, 161

H

Hackers, 273

Hardware Management Console (HMC), 262

Hash algorithms, 224–226, **225**

Health Insurance Portability and Accountability Act (HIPAA), 6, 281, 303

Help desk personnel, role-based access, 314–315

High Availability (HA)

auditing and, 324

row/column access control (RCAC) and, 188

History log, 325–327

Home directories, 210

Host servers, 252

HTTPS, 258, 259

Hypertext Transfer Protocol (HTTP), 257

I

i Access for Windows, 175

i5/OS, 10, **196**

IBM i Access for Web, 253–255, **254**

IBM Navigator for i. *See* Navigator for i

Identification badges, 22

Import files, Copy to Import File (CPYTOIMPF), 207

- Inactivity intervals, system values, 47–49, 47
- INACTTIMO (Inactivity Timeout), 242
- Incident response plan, 393–400
- audit journals and, 396–397, 398
 - data preservation in, 396
 - information gathering in, 395–396
 - investigation in, 396–397
 - law enforcement and, 394
 - preparation for, 393–397
 - proactive response and, 397
 - recreating the system in, 400
 - restoring security data in, 398–400
 - Save Security Data (SAVSECDTA) in, 397
 - security data saved with an object in, 399–400
 - service level agreements (SLAs) and, 395
 - team for, assembling, 394–395
- Independent ASP QSYS.LIB, 195, **196**
- Independent Auxiliary Storage Pools (IASPs), 108
- iNetServer, integrated file system (IFS), 212–213, **212**
- Initial Menu (INLMNU), 101
- Initial Program to Call (INLPGM), 101
- INLMNU, 101
- INLPGM, 101
- Integrated file system (IFS), 195–213, 380–381
- accessing objects in, file shares, 202–205, **203**, **204**, 211–212
 - adopted authority and, 201–202, 205
 - auditing objects in, 202
 - authorities for, 196–202, **197**
 - Change Authority (CHGAUT) in, 198–200, **200**
 - Copy to Import File (CPYTOIMPF) in, 207
 - Copy to Stream File (CPYTOSTMF) in, 207
 - copying objects in, 206–207
 - creating new objects in, 205–206
 - determining appropriate authority for, 209–210
 - Display Authority (DSPAUT) in, 198, 387
- Distributed Data Management (DDM) and, 211
- Document Library Objects (DLOs) in, **196**
- EXCLUDE in, 208–209
- file attributes and, 200–201, **201**
- file ID (FID) and, 202
- file shares in, 202–205, **203**, **204**, 211–212
- file systems in, 195–197, **195–196**
- FTP and, 202, 211
- home directories in, PUBLIC for, 210
- i5/OS file server system in, **196**, 196
- IBM equivalent authorities in, 197
- IBM supplied directories and, PUBLIC authority for, 208–209
- independent ASP QSYS.LIB in, **196**
- iNetServer and, 212–213, **212**
- managing authorities to, 198
- network file system (NFS) in, **196**
- Open Database Connectivity (ODBC) and, 202, 211
- optical file system (QOPT) in, **196**
- oversecuring of, 205
- Portable Applications Solutions Environment (PASE) and, 207
- Print Directory Information (PRTDIRINF) in, 213
- Print Private Authority (PRTPVTAUT) in, 213
- Print Public Authority (PRTPUBAUT) and, 213
- private authorities by IBM in, 205
- PUBLIC authority and, 208–210
- QDLS in, **196**
- QFileSvr.400, **196**
- QOpenSys in, **196**
- QPWFSESERVER authorization list and, 211
- QSYS.LIB in, **196**
- R (Read) authority in, 196
- Retrieve Directory Information (RTVDIRINF) in, 213
- root in, **196**, 209

- RX data authority and, 205
 - Scan File Systems (QSCANFS) in, 207–208
 - Scan File Systems Control (QSCANFSCTL) in, 207–208
 - security recommendations for, 208–213
 - tools for, 213
 - UNIX and, 196
 - user defined file system (UDFS) in, **196**
 - user directories and, PUBLIC authority for, 208–209
 - virus scanning and, 207–208
 - W (Write) authority in, 197
 - Web applications and, QTMHHTTP user profile and, 210
 - Windows NT Server file system (QNTC) in, **196**
 - Work with Authority (WRKAUT) and, 198–200, **199**
 - Work with Object Links (WRKLNK) in, 198
 - X (Execute) authority in, 197
 - Integrity of data, 4–5
 - Internet Assigned Numbers Authority (IANA), 240
 - Internet security, 19–20, 265–282
 - Analyze Default Password (ANZDFTPWD) in, 272
 - business contingency plans and, 282
 - cloud computing and, 278–281
 - controlling access and use in, 273–274
 - corporate security policy and, 267
 - employee infractions of, 267
 - exit points/programs and, 276–277
 - firewalls in, 267, 268–270, **269**
 - hackers and, 273
 - Internet Service Providers (ISPs) and, 268
 - intrusion detection in, 277–278
 - logical partitions (LPARs) in, 269
 - monitoring, 277–281
 - Network Address Translation (NAT) and, 268–269
 - object-level security in, 272–273
 - outsourcing and, 278–281
 - parking of illegal data and, 273
 - process of security development for, 266–267
 - proxy servers in, 270
 - QSECOFR and, 272
 - remote connections and, 267
 - resource security in, 272–273
 - risk assessment in, 265–266
 - risk tolerance levels in, 266–267
 - Save Security Data (SAVSECDTA) in, 272
 - security configuration for, 278
 - social engineering probes and, 268
 - social media and, 267
 - SOCKS servers in, 270
 - system values for, 270–272
 - TCP/IP and, 267, 268–269, 273, 274
 - testing and evaluating, 281
 - uploads/downloads in, 267
 - user profiles and, 273
 - virtual private networks (VPNs) and, 267
 - Web server applications and, 274–276
 - Work with Point to Point TCP/IP (WRKTCPTP) in, 274
 - intranets, 19–20
 - intrusion detection, 277–278
 - IOSYSCFG, **29**, **30**, **98**, 100, 236
 - role-based access and, 314
 - IP addresses, 241
 - IP packet filtering, 241–242
 - iSeries Navigator, 10
 - ISO 27001, 303
 - IT staff
 - classification of data and, 18–19
 - role-based access, 309–321. *See also* Role-based access
- J**
- Java Database Connectivity (JDBC), 290

- networks and connectivity in, 253
 - Job descriptions, application security, 299
 - Job initiation validation, 32
 - Job management
 - Change Job Description (CHGJOB) in, 32
 - Create Job Description (CRTJOB) in, 32
 - job descriptions and, 299
 - JOBACN (Job Action) attribute for, 237
 - system values for, 47–49
 - JOBACN (Job Action) attribute, 237
 - JOBBAS, **330**, 333
 - JOBCHUSR, **330**
 - JOBCTL, **29**, **30**, **98**, 377
 - printers, printed output, and, 217
 - JOBDTA, **330**, 333
 - Journals. *See* Auditing
- K**
- Kerberos, 247, 249
 - Keys, encryption, 223, 224. *See also* Encryption
 - access to, 231
 - asymmetric keys in, 224–226, **225**
 - backing up, 231
 - changing, 231–232
 - disaster recovery considerations and, 233–234
 - generation of, 230
 - hash algorithms in, 224–226, **225**
 - key generation for, 230
 - managing, 230
 - public/private key pairs in, 225
 - storage of, 230–231
 - symmetric keys in, 224–226, **225**
- L**
- LCLPWDGMT (Local Password Management)
 - parameter, 93–94
 - Leaves of absence, 23–24
 - Legal review of security policies, 25
 - Levels of security, 27–38, 376
 - application security and, 298
 - CHGSYSVAL in, 28, 84
 - control-block modification and, 35
 - domain restrictions in, 31–32
 - DSPSYSVAL in, 28
 - job initiation validation in, 32
 - level 20, 28–29, **29**
 - level 30 in, 29–30, **30**
 - level 40 in, 31–34
 - level 50 in, 34–38
 - message restrictions and, 34–35
 - MI instruction restrictions in, 32
 - modified program restoration and, 33
 - moving up to security levels 40 or 50, 36–37
 - parameter-passing validation and, 33
 - pointer removal and, 34–35
 - QSECURITY in, 28
 - QTEMP library maintenance and, 35–36
 - state restrictions in, 31–32
 - system values for, 56
 - Trojan horses and, 33
 - user classes in, 98
 - LIB, 150
 - LIBCRTAUT, 156
 - Libraries, 150
 - Change Library (CHGLIB) in, 43–44
 - Create Library (CRTLIB) in, 43–44
 - Document Library Objects (DLOs) in, **196**
 - object-level security and, 366
 - QSYS.LIB in, **196**
 - Library lists, 299
 - Library-qualified calls, 299–300
 - Licensed Internal Code (LIC), 127
 - "Lifestyle" security, 11
 - Lightweight Directory Access Protocol (LDAP), 239
 - Limiting what users see from the desktop, 252–253

LMTCPB (Limit Capabilities), 102–103
LMTDEVSSN, 104
Locking down system values, 84
Logging, 21. *See also* Auditing
 application security and, 294
 Display Log (DSPLOG) in, 325–327, **325**, **326**
 history log in, 325–327
Logical partitions (LPARs), 269
Logon accounts, 22

M

Make Directory (MKDIR), 380
Management Central, networks and connectivity,
 256
Management support, 10
Masks, column, in RCAC, 185–186
Menu access control, 287–290, **288**
Message restrictions, 34–35
MI instruction restrictions, 32
Microsoft policies, 252
MKDIR, 380
Mobile device security, 250–255
Modified program restoration, 33
Monitoring activity, 21
Monitoring Internet/network security, 277–281

N

Naming conventions, user profiles, 90–91
Navigator for i, 10, 175
 Application Administration in, 175–176, **176**,
 178
 auditing and, 351–352, **351**
 authorities and, 193–194, **194**
 networks and connectivity in, 263, **263**
 object-level security and, 193–194, **194**
 permissions in, 193–194, **194**
 printers, printed output, and spooled files, 222,
 222

 service tools and, 127
 viewing a user's capabilities in, 177, **177**
NETBAS, **330**
NETCLU, **330**
NETCMN, **330**
NETFAIL, **330**
NETSCK, **330**
NETSECURE, **330**
NETTELSVR, **330**
NETUPD, **330**
Network Address Translation (NAT), 242,
 268–269
Network administrator for IBM i, role-based
 access, 314
Network file system (NFS), **196**
Networks and connectivity, 19–20, 235–264. *See*
 also Internet security
 Access Client Solutions (ACS) and, 250–251
 Active Directory and, 239
 Add Community for SNMP
 (ADDCOMSNMP) in, 247
 Add Server Authentication Entry
 (ADDSVRAUTE) in, 248–249, 250
 Analyze Default Password (ANZDFTPWD)
 in, 272
 anonymous FTP and, 243
 Application Administration and, 252
 application security and, 298
 attributes for, 237
 AUTOSTART values and, 239
 business contingency plans and, 282
 Certificate Authorities (CA) in, 257, 258–261
 Change Command Default (CHGCMDDFT)
 in, 239
 Change DDM TCP/IP Attributes
 (CHGDDMTCPA) in, 248
 Change FTP Attribute (CHGFTPA) in, 239
 Change Function Usage (CHGFCNUSG) in,
 252

- cloud computing and, 278–281
- community names in, 247
- Configure TCP/IP (CFGTCP) in, 240
- data transfer issues in, 251
- DDMACC (DDM Access) attribute for, 237, 238
- Digital Certificate Manager (DCM) in, 258, 261
- digital certificates in, 257, 258
- Display Function Usage (DSPFCNUSG) in, 252
- Distributed Data Management (DDM) in, 247–250
- Distributed Relational Database Architecture (DRDA) and, 238, 247–250
- Domain Name Service (DNS) in, 246
- encryption and, 257–262
- End Host Server (ENDHOSTSVR) in, 252
- End TCP/IP (ENDTCP) in, 252
- Enterprise Identity Mapping (EIM) and, 249
- exit points/programs and, 255–256, 276–277
- firewalls and, 268–270, **269**
- FTP and, 241, 242–244, **243**, 257
- Group Policy Objects (GPOs) in, 252–253
- host servers and, 252
- HTTPS in, 258, 259
- Hypertext Transfer Protocol (HTTP) and, 257
- IBM i Access for Web and, 253–255, **254**
- INACTTIMO (Inactivity Timeout) in, 242
- internal addresses and, 241
- intrusion detection in, 277–278
- IOSYSCFG special authority and, 236
- IP packet filtering and, 241–242
- Java Database Connectivity (JDBC) and, 253
- JOBACN (Job Action) attribute for, 237
- Kerberos in, 249
- Lightweight Directory Access Protocol (LDAP) and, 239
- limiting what users see from the desktop in, 252–253
- logical partitions (LPARs) in, 269
- Management Central in, 256
- Microsoft policies and, 252
- monitoring, 277–281
- Navigator for i and, 263, **263**
- Network Address Translation (NAT) and, 242, 268–269
- Open Database Connectivity (ODBC) and, 250, 253
- outsourcing and, 278–281
- password substitution and, 250
- PC and mobile devices in, 250–255
- PCSACC (PC Support Access) attribute for, 237, 238
- physical security and, 235–236
- ports in, 240–241
- Post Office Protocol (POP) in, 245–246
- proxy servers in, 270
- QAUTOCFG (Automatic Device Configuration) system value for, 236
- QAUTOVRT (Automatic Config of Virtual Devices) system value for, 236
- QINACTITV (Inactivity Time Out Interval) in, 240
- QMAXSGNACN (Maximum Sign-on Action) in, 242
- QMAXSIGN (Maximum Number of Sign-on Attempts) in, 242
- QRETSVRSEC (Retain Server Security) in, 249
- QSECOFR and, 272
- QSSLCSL and, **260**
- QSSLCSLCTL and, **259**
- QSSLPCL and **260**
- Registration Facility and, 255
- remote command issues in, 251
- Remote Execution (REXEC) and, 246–247
- Save Security Data (SAVSECDTA) in, 256, 272
- secure communications and, 256–262

Secure Shell (SSH) in, 262
Secure Sockets Layer (SSL) in, 257–262
security configuration for, 278
security policies and, 19–20
selective install feature in, 253
session time-out values in, 240
Simple Mail Transfer Protocol (SMTP) in,
244–245
Simple Network Management Protocol
(SNMP) and, 247
Simple Network Time Protocol (SNTP) in, 247
sniffers in, 262
SOCKS servers in, 270
Start TCP/IP (STRTCP) in, 239–240
Start TCP/IP Servers (STRTCPSVR) in,
239–240
system values for, 236, 270–272
Systems Network Architecture (SNA) and, 237
Systems Network Architecture Distribution
Services (SNADS) and, 238
TCP/IP and, 235, 238–250, 268–269, 273, 274
Telnet and, 241, 257
tools for, 263
Transport Layer Security (TLS) in, 257–262
User Datagram Protocol (UDP) and, 241
virtual private networks (VPNs) and, 261
Web server applications and, 274–276
wireless considerations in, 262–263
Work with Function Usage (WRKFCNUSG)
in, 252
Work with Names for SMTP
(WRKNAMSMTP) in, 245
Work with Point to Point TCP/IP
(WRKTCPPPTP) in, 274
Work with Registration Information
(WRKREGINF) in, 255, 263
Work with System Values (WRKSYSVAL) in,
255
NONE, **98**
Notification of security policies, 22–23

O

OBJALTER, **148**, 150, **152**, **197**
OBJAUD (Object Auditing), 335–338, 339
Object authorities, 148, 149–150
Object-level security, 147–194, 353–374. *See*
also Object management
access control and, 358
ACCTNG profile and, 355
ADD in, 150–151
adopted authorities and, 362–363
adopted authority and, 166–170, **167**
ALLOBJ and, 147
application security and, 368–371
architecture issues and, 355–356
auditing and, 335–338
auditing to collect information on, 358–360
authorities and, 362
authority cache and, 166
authority checking in, 162–166, **163**, **165**
authority collection in, 189–193
authority groupings and, 152–153
authority relationships and, 151–152
authorization lists in, 160–162, **160**, 364–365
backup and recovery and, 371–373
“big picture” concepts in, 356–361, **357**
Change Function Usage (CHGFCNUSG) in,
178
Change Object Owner (CHGOBJOWN) in,
172–174
Change Object Primary Group (CHGOBJPGP)
in, 155
compliance issues and, 387
compliance with, 373
Create Authority (CRTAUT) in, 156–160
data authorities and, 148, 150–151
debugging and, 371–373
decision points in, 362–368
default public authority and, 158–160
design considerations and, 355

- Display Function Usage (DSPFCNUSG) in, 178
- Display Object Authority (DSPOBJAUT) in, 155, 186, 379, 387
- DLT in, 151–152
- Dynamic SQL and, 361
- Edit Object Authority (EDTOBJAUT) in, 148, 155, 161, 186
- EXCLUDE and, 153, 158–160, 163
- EXECUTE in, 151, 152
- Grant Object Authority (GRTOBJAUT) in, 148, 153, 160, 161
- group profiles and, 153–155
- implementation of, 353–374
- information collection for implementation of, 358–360
- Internet security and, 272–273
- issues to watch for in, 373–374
- libraries and, 366
- limited user function (application administration) and, 174–179, **176, 177, 178**
- Navigator for i and, 193–194, **194**
- new objects and, 338
- OBJALTER in, 150
- object authorities in, 149–150
- OBJEXIST in, 149–150
- OBJMGT in, 149–150
- OBJOPR in, 149–150
- OBJREF in, 150
- obsolete object removal, 375–376
- ownership of objects in, 172–174, 362
- permissions in, Navigator for i and, 193–194, **194**
- Print SQL Information (PRTSQLINF) in, 361
- private authorities and, 148–153
- PUBLIC and, 364, 365, 366–367
- PUBLIC authority in, 155–160, 163–165
- QCRTAUT in, 156–160
- queries and, 367–368
- READ in, 150–151
- Revoke Object Authority (RVKOBJAUT) in, 148, 161
- rolling out changes to, 370–371
- row and column access control (RCAC) and, 179–188
- Save/Restore functions and, 170–172
- scope of, 354–355
- security data saved with an object in, 399–400
- tools to manage authorities and, 193
- UPD in, 150–151
- User Function Registration APIs in, 175
- user profiles and, 355–356
- vendors and, 373
- viewing a user’s capabilities in, 177, **177**
- Work with Function Usage (WRKFCNUSG) in, 178
- Work with Objects by Primary Group (WRKOBJPGP) in, 155
- Object management
 - Allow Object Differences (ALWOBJDIF) in, 33
 - auditing for new, QCRTOBJAUD, 83–84
 - copying objects in, 206–207
 - creating objects in, 205–206
 - Group Policy Objects (GPOs) in, 252–253
 - Restore Object (RSTOBJ) in, 33
 - system values for, 45–47, 57–58
 - Work with Object Links (WRKLNK) in, 198
- OBJEXIST, **148, 149–150, 152, 197**
- OBJMGT, **148, 149–150, 152, 197, 330, 379**
- OBJOPR, **148, 149–150, 152, 197, 379**
- OBJREF, **148, 150, 152, 197**
- Obsolete object removal, 375–376
- ODBC, 181, 183
- Open Database Connectivity (ODBC), 7, 8, 250, 290
 - integrated file system (IFS) and, 202, 211
 - networks and connectivity in, 253

OpenSSH, 262
Operating systems, 10
Operations Console, 139–141
Operator role, QSYSOPR, 311–314
OPRCTL (Operator Control) parameter, 217
Optical file system (QOPT), **196**
OPTICAL, **330**
OS/400, 10
Output queues (printer), 150, 216–222. *See also*
 Printers and printed output
OUTQ, 150
Outsourcing, Internet security, 278–281
OWNER, 104–107
Ownership of applications, 293
Ownership of data, classification of data, 18
Ownership of objects, 172–174, 362

P

Packet filtering, 241–242
Parameter-passing validation, 33
Parking of illegal data, 273
PASSWORD parameter, user profiles, 91–93
Password substitution, 250
Passwords, 22, 130
 adjacent digit limits on, QPWDLMTAJC, 63
 Analyze Default Password (ANZDFTPWD)
 in, 93, 110, 272, 386
 application security and, 297, 300
 Block Password Change (PWDCHGBLK) in,
 95
 block changes in, QPWDCHGBLK, 71, 74–75
 case-sensitivity in, 130, 131
 Change Password (CHGPWD) in, 60, 378
 Change Password (QSYSCHGPW) in, 60, 95
 changing policies for, 132
 choosing a policy for, 132
 clear text, 300
 Data Encryption Standard (DES), 129
 default values for, 92
 expiration interval for, PWDEXPITV in,
 94–95
 expiration interval for, QPWDEXPITV, 62–63
 expiration of, 130, 131
 expiration of, PWDEXP parameter in, 93
 expiration warning for, QPWDEXPWRN, 71,
 75
 IBM-supplied user profiles (Qxxx) and, 92–93
 levels of, QPWDLVL, 61–62
 Local Password Management
 (LCLPWDMGT) in, 93–94
 maximum number of characters in,
 QPWDMAXLEN, 65–66
 maximum sign-on attempts with, 131
 minimum number of characters in,
 QPWDMINLEN, 65–66
 PASSWORD parameter for user profiles in,
 91–93
 position of characters in, QPWDPOSIF,
 66–67
 QPWDBLKPWD, 378
 repeating character limits in, QPWDLMTREP,
 64–65
 repetition of, 131
 require different password for,
 QPWDRQDDIF, 67–68
 require digit in, QPWDRQDDGT, 67
 rules for, QPWDRULES, 71–74, 92
 Secure Hash Algorithm (SHA) in, 130
 service tools and, 129–132
 specific character limits in, QPWDLMTCHR,
 64
 storage of, 300
 substitution, 250
 system values for, 60–75, **60–61**
 V6R1 system values for, 71–75
 validation program for, QPWDVLDPGM,
 68–71

- Payment Card Industry Data Security Standard (PCI DSS), 14, 226, 281, 285, 303, 386, 387
- PC security
 - limiting what users see from the desktop in, 252–253
 - networks and connectivity in, 250–255
 - selective install feature in, 253
- PCSACC (PC Support Access) attribute, 237, 238
- PGMADP, **330**, 333
- PGMFAIL, **330**
- PGMR, **29**, **30**, 97, **98**
- Physical security, 14–15
 - networks and connectivity in, 235–236
- Platform-specific issues in security policies, 21
- Pointer removal, 34–35
- Policies. *See* Security policies and procedures
- Portable Applications Solutions Environment (PASE), 207
- Ports, networks and connectivity, 240–241
- Post Office Protocol (POP), 245–246
- Preserving data, incident response, 396
- Print Adopting Objects (PRTADPOBJ), 193
- Print Directory Information (PRTDIRINF), 213
- Print Private Authorities (PRTPVTAUT), 193, 213, 387
- Print Profile Internals (PRTPRFINT), 110
- Print Public Authorities (PRTPUBAUT), 193, 213, 387
- Print Queue Authority Report (PRTQAUT), 222
- Print SQL Information (PRTSQLINF), 361
- Print System Security Attributes (PRTSYSSECA), 84
- Print User Profile (PRTUSRPRF), 110, 386
- Print Validation List (PRTVLDL), 114–123, **124**
- Printers and printed output, 215–222
 - AUT (Authority) in, 218
 - AUTCHK (Authority Check) parameter in, 217–218
 - authorities required for, 218–219, **219**
 - Change Output Queue (CHGOUTQ) in, 216
 - Copy Spooled File (CPYSPLF) in, 216, 219
 - Create Output Queue (CRTOUTQ) in, 216–218, 220–222
 - CRTOUTQ parameters for, 216–218
 - Display Spooled File (DSPSPLF) in, 219
 - DSPDATA (Display Data) parameter for, 216–217
 - JOBCTL authority and, 217
 - Navigator for i and, 222, **222**
 - OPRCTL (Operator Control) parameter in, 217
 - output queue security for, 216–222
 - ownership of output queue in, 219–220
 - Print Queue Authority Report (PRTQAUT) in, 222
 - sample security implementation for, 220–222
 - Send TCP/IP Spooled File (SNDTCPSPLF) in, 216
 - SPLCTL special authority in, 218
 - tools for, 222
 - Work with Output Queue (WRKOUTQ) in, 218
 - Work with Output Queue Description (WRKOUTQD) in, 216
 - Work with Spooled Files (WRKSPLF) in, 218
- Privacy issues, 5–6, 17
- Private authorities, 109, 148–153. *See also* Authorities
 - user profiles and, 109
- Profile-swap APIs, 292
- Profile-token APIs, 292
- Programmer/analyst role, role-based access, 315–318
- Proxy servers, 270
- PRTADPOBJ, 193
- PRTDIRINF, 213

- PRTDTA, **330**, 333
- PRTPRFINT, 110
- PRTPUBAUT, 193, 213, 387
- PRTPVTAUT, 193, 213, 387
- PRTQAUT, 222
- PRTSQLINF, 361
- PRTUSRPRF, 110, 386
- PRTVLDL, 114–123, **124**
- PTFOBJ, **330**
- PTFOPR, **330**, 331, 332, 339
- PUBLIC, 21, 108–109, 155–160, 163–165, 364, 365, 366–367, 380
 - application security and, 289, 296, 298
 - integrated file system (IFS) and, 208–210
 - limited user function (application administration) and, 174–179, **176**, **177**, **178**
- Public data, 17
- Public key infrastructure (PKI), 224–226, **225**
- Public/private key pairs, 225
- PWDCHGBLK (Block Password Change), 95, 104
- PWDEXP (Set Password to Expire) parameter, 93
- PWDEXPITV (Password Expiration Interval), 94–95, 104

- Q**
- QALWOBJRST, **38**, 40
- QALWUSRDMN, **38**, 41
- QAUDCTL (Auditing Control), **76**, 329, 339, 376
- QAUDENDACN, 77
- QAUDENDACN, **76**, 339
- QAUDFRCLVL (Auditing Force Level), **76**, 78, 329, 339
- QAUDLVL (Auditing Level), **76**, 78–82, 317, 329–333, **330–331**, 339, 340, 341, 376
- QAUDLVL2 (Auditing Level Extension), **76**, 82, 329–333, **330–331**
- QAUJRN, 341
- QAUTOCFG (Automatic Device Configuration), **38**, 42, 236
- QAUTOVRT (Automatic Config of Virtual Devices), **38**, 42–43, 236
- QCMD, 35
- QCONSOLE, device profiles, 140
- QCRTAUT (Create Authority), **38**, 43–44, 156–160, 338
- QCRTOBJAUD (Auditing for New Objects), **76**, 83–84, 338
- QDLS, **196**
- QDSCJOBITV, **38**, 47–49
- QDSPSGNINE, **38**, 44–45, 104
- QFileSvr.400, **196**
- QFRCCVNRST, **38**, 45–47
- QHSTLOGSIZ (History Log Size), 326
- QINACTITV (Inactivity Time Out Interval), **38**, 47–49, 240
- QINACTMSGQ, **38**, 47–49
- QLMTDEVSSN, **38**, 49–50, 104
- QLMTSECOFR, **39**, 50–51
- QMAXSGNACN (Maximum Sign-on Action), **39**, 51–52, 96, 242
- QMAXSIGN (Maximum Number of Sign-on Attempts), **39**, 51–52, 96, 242
- QNTC, **196**
- QOpenSys, **196**
- QOPT, **196**
- QPGMR, 92
 - role-based access and, 315–318
- QPWDBLKPWD, 378
- QPWDCHGBLK, **60**, 71, 74–75, 104
- QPWDEXPITV, **60**, 62–63, 104, 376
- QPWDEXPWRN, **60**, 71, 75
- QPWDLMTAJC, **60**, 63

- QPWDLMTCHR, **60**, 64
 QPWDLMTREP, **60**, 64–65
 QPWDLVL, **61**, 376
 QPWDMAXLEN, **61**, 65–66
 QPWDMINLEN, **61**, 65–66
 QPWDPOSDIF, **61**, 66–67
 QPWDRQDDGT, **61**, 67
 QPWDRQDDIF, **61**, 67–68
 QPWDRULES, **61**, 71–74, 92
 QPWDVLDPGM, **61**, 68–71
 QRETSVRSEC (Retain Server Security), **39**, 53,
 125,
 249
 QRMTSIGN, **39**, 54
 QSCANFS, **39**, 55–56, 207–208
 QSCANFSCTL, **39**, 55–56, 207–208
 QSECOFR, 31, 93, 332, 379
 adopted authority and, 170
 application security and, 296, 297
 auditing and, 333
 compliance issues and, 385
 disabled, 96
 Internet security and, 272
 ownership of objects and, 174
 role-based access and, 318–319
 service tools and, 128, **136–137**, 138
 user profiles and, 86
 QSECURITY, 28, 39, **39**, 56, 376
 QSRV, 92
 service tools and, **136–137**
 QSRVBAS, 92
 QSSCLSL, **39**, 59, **260**
 QSSCLSLCTL, **39**, 59, **259**
 QSSLPCL **39**, 59, **260**
 QSYS, 31
 QSYS.LIB, **196**
 QSYSCHGPW, 60, 95
 QSYSOPR, 92
 role-based access and, 311–314
 QTEMP, 35–36, 41
 QTMHHTTP user profile, 210
 queries, object-level security, 367–368
 QUSEADPAUT, **39**, 56–57
 QUSER, 92
 QVfyOBRST, **39**, 57–58
 Qxxx user profiles, 92–93
- R**
- R (Read) authority, 196
 RC5, 225
 READ, **148**, 150–151, **152**, **197**, 379
 Recovery. *See* Backup and recovery; Incident
 response plan
 Recreating the system after a breach, 400
 Registration Facility, Work with Registration
 Information (WRKREGINF), 255, 263
 Remote command issues, 251
 Remote connections, 267
 Remote Execution (REXEC), 246–247
 Remote sign-on, 54
 Resource security, 29, 272–273
 Response plan. *See* Incident response plan
 Responsible parties, in security policies, 15
 Restore Authority (RSTAUT), 154, 398, 399
 Restore Object (RSTOBJ), 33
 Restore User Profile (RSTUSRPRF), 398, 399
 Restoring security data, 398–400
 Restricted data, 17
 Retain Server Security (QRETSVRSEC), 125
 Retention of data, 16, 18
 Retrieve Directory Information (RTVDIRINF),
 213
 Reviewing requirements for security, 9, 379–380,
 389–391
 Revoke Object Authority (RVKOBJAUT), 148,
 161

- Risk assessment/evaluation, 3–6, 10, 265–266, 284–285, 388–389
- Risk tolerance, 266–267
- Role-based access, 104, 303–321
 - ALLOBJ and, 317–318
 - Change User Audit (CHGUSRAUD) in, 317, 340
 - compliance issues and, 303
 - consultants in, 319–321
 - defining a secure environment for each business function in, 311
 - group profiles and, 305–308
 - help desk personnel in, SECADM and, 314–315
 - implementation of, 308–309
 - IOSYSCFG in, 314
 - IT personnel in, 309–321
 - network administrator for IBM I in, 314
 - operator role in, QSYSOPR and, 311–314
 - programmer/analyst role in, QPGMR and, 315–318
 - QAUDLVL (Auditing Level) and, 317
 - roles in, 303–305, 310, **310–311**
 - security administrators in, QSECOFR and, 318–319
 - system administrators in, QSECOFR and, 318–319
 - vendors in, 319–321
- Roles, 286–287, 303–305, 310, **310–311**
- Root, **196**, 209
- Row and column access control (RCAC), 179–188
 - ALLOBJ and, 180, 181, 184–185
 - BOSS option 47 in, 179
 - column masks, 185–186
 - Display Object Authority (DSPOBJAUT) in, 186–187, **187**
 - High Availability (HA) systems and, 188
 - how it works, 181–182
 - information and IBM resources for, 188
 - managing, 186–187, **187**
 - permissions in, 183–184
 - prerequisites for, 179
 - programmer considerations in, 184–185
 - Save/Restore considerations in, 187–188
 - SECADM and, 179, 180, 181
 - security settings in, 179–181, **180**
- RSA, 225
- RSTAUT, 154, 398, 399
- RSTOBJ, 33
- RSTUSRPRF, 398, 399
- RTVDIRINF, 213
- Run Query (RUNQRY), 181–182, 183
- RVKOBJAUT, 148, 161
- RX data authority, 205
- S**
- SANS Institute, 25
- Sarbanes-Oxley Act (SOX), 303, 309, 323
- Save Security Data (SAVSECDTA), 154, 192, 256, 272, 397
- Save/Restore
 - authorities and, 170–172
 - row/column access control (RCAC) and, 187–188
- SAVRST, **330**, 331, 332, 339
- SAVSECDTA, 154, 192, 256, 272, 397
- SAVSYS, **29**, **30**, **98**, 100, 377, 380
- Scan File Systems (QSCANFS), 207–208
- Scan File Systems Control (QSCANFCTL), 207–208
- Scope of security project, 354–355
- SECADM, **29**, **30**, 97, **98**, 100
 - adopted authority and, 166–170, **167**
 - authority collection and, 192
 - compliance issues and, 385
 - role-based access and, 314–315
 - row/column access control (RCAC) and, 179, 180, 181

- user profiles and, 86
- SECBATCH tools, 109, 193, **193**
- SECCFG, 331, **331**, 333, 339
- SECDIRSRV, **331**
- SECIPC, **331**
- SECNAS, **331**
- SECOFR, **29**, **30**, 97, **98**
- SECRUN, 331, **331**, 333, 339
- SECSCKD, **331**, 331
- SECTOOLS tools, 109, 193, **193**
- Secure Hash Algorithm (SHA), 130
- Secure Shell (SSH), 262
- Secure Sockets Layer (SSL), 257–262
 - device profiles and, 139
 - system values for, 59
- SECURITY, 333
- Security administration, 375–381
 - access control issues in, 380
 - authority management in, 379
 - integrated file system (IFS) and, 380–381
 - keeping current in, 381
 - obsolete object removal in, 375–376
 - PTFs relevant to, 381
 - QSECOFR in, 318–319
 - reviewing security in, 379–380
 - system values setting and, 376
 - user profile issues in, 376–379
- Security assessment, 388–389
- Security awareness program, 401–405
 - Chief Security Officer (CSO) in, 401
 - communicating importance of security in, 402–403
 - getting started with, 403–405
 - issues to address in, 404–405
 - training for, 401–402
- Security data saved with an object, 399–400
- Security incident response plan. *See* Incident response plan
- Security level 20, 28–29, **29**
- Security level 30, 29–30, **30**
- Security level 40, 31–34
 - job initiation validation in, 32
 - MI instruction restrictions in, 32
 - modified program restoration and, 33
 - moving to, 36–37
 - parameter-passing validation and, 33
 - state and domain restrictions in, 31–32
 - Trojan horses and, 33
- Security level 50, 34–38
 - control-block modification and, 35
 - message restrictions and, 34–35
 - moving to, 36–37
 - pointer removal and, 34–35
 - QTEMP library maintenance and, 35–36
- Security policies and procedures, 7, 10, 11, 13–25
 - application design and, 20
 - Bring Your Own Device (BYOD) and, 20–21
 - business events and procedures in, 23–24
 - classification of data in, 15–19
 - compliance issues, 14
 - “corporate memory” and, 14
 - currency of and updating, 24
 - documents for, 14
 - employee guidelines in, 21–22
 - essential items only in, 24
 - generic quality of, 24
 - Internet security and, 267
 - legal review of, 25
 - management support for, 14
 - Microsoft policies and, 252
 - network connections and, 19–20
 - notification, enforcement, compliance with, 22–23
 - physical security issues in, 14–15
 - platform-specific issues and, 21
 - responsible parties to, 15
 - “rules” and, 13
 - social media and, 21

- templates for, 25
- terminations/firings and, 23–24
- SECURITY, **330**
- SECVFY, **331**
- SECVLDL, **331**
- Selective install feature, 253
- Send TCP/IP Spooled File (SNDTCPSPLF), 216
- Server security. *See also* Networks and connectivity
 - Add Server Authentication Entry (ADDSVRAUTE) in, 248–249, 250
 - End Host Server (ENDHOSTSVR) in, 252
 - End TCP/IP (ENDTCP) in, 252
 - exit points and, 255–256
 - host, 252
 - proxy servers in, 270
 - QRETSVRSEC (Retain Server Security) in, 249
 - Retain Server Security (QRETSVRSEC) in, 125
 - SOCKS servers in, 270
 - Start TCP/IP Servers (STRTCPSVR) in, 239–240
 - system values for, 53
- SERVICE, 100, 101, 331, 333, 339
- Service functions, 127
- Service level agreements (SLAs), 395
- Service tools, 127–145
 - auditing (monitoring) of, 143
 - Change Service Tools User Privileges in, 133–136, **133, 134**
 - changing password policies for, 132
 - Copy Audit Journal Entries (CPYAUDJRNE) in, 143
 - Create Service Tools User ID in, **129**
 - Dedicated Service Tools (DST) in, 127, 142–144
 - default password policy for, 130–131
 - device profiles and, 139–141
 - Display Service Tools User ID in, 138, **139**
 - features of, 138
 - functional privileges in, 128, 132–137, **136–137, 136**
 - IBM Navigator for i and, 127
 - IBM security resources for, 145
 - monitoring use of, 142–144
 - passwords for service tool user IDs, 129–132
 - predefined user IDs for, 130, 131
 - QCONSOLE and, 140
 - QSECOFR and, 128, **136–137, 138**
 - QSRV in, **136–137**
 - security recommendations for, 144–145
 - service functions and, 127
 - service tools user identities in, 128–132
 - Start System Service Tools (STRSST) in, 127
 - System Service Tools (SST) in, 127
 - Work with Service Tools Security Data in, 140
 - Work with Service Tools User IDs in, **129, 129**
 - Work with System Security panel in, 141–142, **141**
- Service tools user identities, 85, 127, 128–132
- SERVICE, **29, 30, 98, 331**
- Session management, system values, 49–50
- Session time-out values, networks and connectivity, 240
- Share, file shares, 202–205, **203, 204**, 211–212
- Sign-on security, 101–103
 - Change User Profile (CHGPRF) in, 102
 - Current Library (CURLIB) in, 101
 - Initial Menu (INLMNU) and, 101
 - Initial Program to Call (INLPGM) and, 101
 - LMTCPB (Limit Capabilities) and, 102–103
 - maximum attempts at, 131
 - options for, 101–103
 - system values for, 44–45, 51–52, 54, 96
 - user profiles and, 101–103
- Simple Mail Transfer Protocol (SMTP), 244–245
- Simple Network Management Protocol (SNMP), 247

- Simple Network Time Protocol (SNTP), 247
- SNDTCPSPLF, 216
- Sniffers, wireless, 262
- Social engineering probes, 268
- Social media, 21, 22
 - Internet security and, 267
- SOCKS servers, 270
- SPCAUT (Special Authority), 97–101
- SPLCTL special authority, **29, 30, 98**, 100, 218, 377
- SPLFDTA, **331**, 333
- Spooled files
 - Copy Spooled File (CPYSPLF) in, 216, 219
 - Display Spooled File (DSPSPLF) in, 219
 - Navigator for i and, 222, **222**
 - Send TCP/IP Spooled File (SNDTCPSPLF) in, 216
 - Work with Spooled Files (WRKSPLF) in, 218
- SQL, 182
 - authority collection in, 190, **190**
- Start Authority Collection (STRAUTCOL), 189–190, **190**
- Start Pass Through (STRPASTHR), 54
- Start System Service Tools (STRSST), 127
- Start TCP/IP (STRTCP), 239–240
- Start TCP/IP Servers (STRTCPSVR), 239–240
- State restrictions, 31–32
- STATUS (Profile Status), 96
- Strategic issues, 7–9
- STRAUTCOL, 189–190, **190**
- Stream files, Copy to Stream File (CPYTOSTMF), 207
- STRPASTHR, 54
- STRSST, 127
- STRTCP, 239–240
- STRTCPSVR, 239–240
- SUPGRPPRF (Supplemental Groups), 104, 154
- Symmetric keys, 224–226, **225**
- SYSMGT, **331**
- SYSOPR, **29, 30, 98**, 97
- SYSTEM, 34
- System administrators, QSECOFR, 318–319
- System-level security, 27–84
 - auditing and, 75–84, **76**
 - CHGSYSVAL in, 28, 84
 - Common Criteria and, 41
 - Common Criteria for Information Tech Security Evaluation and, 27
 - DSPSYSVAL in, 28
 - general system values in, 38–60
 - levels of, 27–38
 - locking down system values for, 84
 - online guide to system values for, 39
 - passwords in, 60–75, **60–61**
 - Print System Security Attributes (PRTSYSSECA) for, 84
 - QSECURITY in, 28
 - resource security in, 29
 - system values in, 27, 37–84
- System Service Tools (SST), 127
- System Service Tools (SSTs), 297
- System values, 376
 - application security and, 297
 - auditing and, 329–333, **330–331**, 329
 - compliance issues and, 385
 - Display System Values (DSPSYSVAL) in, 385
 - general, 38–60, 38
 - Internet security and, 270–272, 270
 - locking down, 84
 - networks and connectivity in, 236
 - online guide to, 39
 - overrides for, 104
 - password related, 60–75, **60–61**, 60
 - Print System Security Attributes (PRTSYSSECA) for, 84
 - Work with System Values (WRKSYSVAL) in, 255

System values, 27–84. *See also* System-level security; *See also* specific system values
System-wide auditing, 329–333
Systems Network Architecture (SNA), 237
Systems Network Architecture Distribution Services (SNADS), 238

T

TCP/IP, 235, 238–250, 268–269. *See also* Internet security; Networks and connectivity
Telnet, 42, 241, 257
Templates for user profiles, 376
Terminations/firings, 23–24
Threat evaluation, 7
Time, Simple Network Time Protocol (SNTP) in o, 247
Time-out intervals
 networks and connectivity in, 240
 system values for, 47–49
Top secret data, 15–19
Training for security, 401–402
Transfers of employees, 23–24
Transport Layer Security (TLS), 59, 225, 257–262
Triple DES, 225
Trojan horses, 33, 299

U

UNIX, integrated file system (IFS), 196
UPD, **148**, 150–151, **152**, **197**, 379
Update Data (UPDDTA), 182
Uploads/downloads, 267
USE, 379
Use Adopted Authority (USEADPAUT), 168
USER, 32, 34, 97, 156
User Datagram Protocol (UDP), 241

User defined file system (UDFS), **196**, 195
User directories, integrated file system (IFS) and PUBLIC authority, 208–209
User Function Registration APIs, 175
User Identification (UID), 108
User IDs, 292–293
User profiles, 85–125, 192, 292–293, 376–379.
 See also Role-based access; Validation list users
 ACCTNG profile and, 355
 Active Directory and, 90
 ANZPRFACT (Analyze Profile Activity), 110
 application security and, 292–293, 294–295, 297
 assigning to a group, 106–107
 attributes for, 87–89
 AUT (Authority) in, 108–109
 authority checking and, 165–166, **165**
 authority collection and, 192
 Change Activation Schedule Entry (CHGACTSCDE) in, 110
 Change Active Profiles List (CHGACTPRFL) in, 110
 Change Expiration Schedule Entry (CHGEXPSCDE) in, 110
 Change User Profile (CHGUSRPRF) in, 52, 87, 102, 168, 292
 classes of users and, 97–101
 compliance issues and, 385
 copying, 112–113
 Create User Profile (CRTUSRPRF) in, 87–89, 105, 192, 334
 creating, with Navigator for i instead of CRTUSRPRF, 111–112, **111**
 definition of, 86
 Delete User Profile (DLTUSRPRF) in, 87
 device profiles and, 139–141
 Display Activation Schedule (DSPACTSCD) in, 110

- Display Active Profiles List (DSPACTPRFL)
 - in, 110
 - Display Authorized Users (DSPAUTUSR) in, 386
 - Display Expiration Schedule (DSPEXPSCD)
 - in, 110
 - Display User Profile (DSPUSRPRF) in, 192, 378, 386
 - dynamic SQL and, 170
 - FTP and, 85
 - Group Identification Number (GID) in, 108
 - group profiles and, 104–109, 153–155, 305–308, 379
 - IBM supplied (Qxxx), 92–93
 - Independent Auxiliary Storage Pools (IASPs)
 - in, 108
 - Internet security and, 273
 - IOSYSCFG and, 100
 - LCLPWDMGT (Local Password Management) parameter in, 93–94
 - levels of security and, user classes, 98
 - naming schemes used in, 90–91
 - object-level security and, 355–356
 - PASSWORD in, 91–93
 - Print Profile Internals (PRTPRFINT) in, 110
 - Print User Profile (PRTUSRPRF) in, 110, 386
 - Print Validation List (PRTVLDL) in, 114–123, **124**
 - private authorities and, 109
 - PWDCHGBLK (Block Password Change) in, 95
 - PWDEXP (Set Password to Expire) parameter in, 93
 - PWDEXPITV (Password Expiration Interval)
 - in, 94–95
 - QSECOFR and, 86, 96
 - Restore User Profile (RSTUSRPRF) in, 398, 399
 - Retain Server Security (QRETSVRSEC) in, 125
 - role-based access and, 104
 - SAVSYS and, 100
 - SECADM and, 86, 100
 - security implications of, 124–125
 - SERVICE and, 100, 101
 - service tools user identities and, 85, 127, 128–132. *See also* Service tools, 128
 - sign-on options and, 101–103
 - SPCAUT (Special Authority) in, 97–101
 - SPLCTL and, 100
 - STATUS (Profile Status) in, 96
 - system value overrides in, 104
 - templates for, 376
 - tools for, 109, **109–110**
 - User Identification (UID) in, 108
 - uses for, 86
 - USRCLS (User Class) in, 97–101
 - USREXPDATE (User Expiration Date) in, 108
 - USREXPITV (User Expiration Interval) in, 108
 - USRPRF parameter for, 89–91
 - validation list users and, 85, 113–125
 - USER, 29, 30, 98**
 - USRCLS (User Class), 97–101, **98**
 - USREXPDATE (User Expiration Date), 108
 - USREXPITV (User Expiration Interval), 108
 - USRPRF parameter, 89–91
- V**
- V6R1, system values, 71–75
 - V7R3, new features, **78–80, 82**, 189, **330–331**, 360
 - Validation, passwords, QPWDVLDPGM, 68–71
 - Validation list users, 85, 113–125. *See also* User profiles
 - Vendors
 - application security and, 297
 - object-level security and, 373

- role-based access and, 319–321
- Verification, system values, 57–58
- Virtual private networks (VPNs), 19–20, 261
 - encryption and, 226
 - Internet security and, 267
- Virus scanning, integrated file system (IFS), 207–208

W

- W (Write) authority, 197
- Web applications
 - integrated file system (IFS) and, QTMHHTTP user profile and, 210
- Web server applications, 274–276
- Windows NT Server file system (QNTC), **196**
- Wireless networks, 19–20, 262–263
- Work with Authority (WRKAUT), 198–200, **199**
- Work with Function Usage (WRKFCNUSG), 178, 252
- Work with Names for SMTP (WRKNAMSMTP), 245
- Work with Object Links (WRKLNK), 198
- Work with Objects by Primary Group (WRKOBJPGP), 155
- Work with Output Queue (WRKOUTQ), 218

- Work with Output Queue Description (WRKOUTQD), 216
- Work with Point to Point TCP/IP (WRKTCPPPTP), 274
- Work with Registration Information (WRKREGINF), 255, 263
- Work with Service Tools Security Data, 140
- Work with Service Tools User IDs, **129**, 129
- Work with Spooled Files (WRKSPLF), 218
- Work with System Security panel, 141–142, **141**
- Work with System Values (WRKSYSVAL), 255
- Workstation management, system values, 49–51
- WRKAUT, 198–200, **199**
- WRKFCNUSG, 178, 252
- WRKLNK, 198
- WRKOBJPGP, 155
- WRKOUTQ, 218
- WRKOUTQD, 216
- WRKREGINF, 255, 263
- WRKSPLF, 218
- WRKSYSVAL, 255
- WRKTCPPPTP, 274

X

- X (Execute) authority, 197