Abuse, 63
destruction, 63
disruption, 63
modification, 63
privacy violation, 63
theft, 63
unauthorized use, 63
Acceptability tests, 172
Daubert reliability test, 172
factors, 172
false positives, 172
purpose of, 172
Access control, 10
application, 49
checklist, logical access, 211
checklist, physical access, 260
log review, 189
network, 32–38, 48
operating system, 48
purpose, 10
software, 48–50
Access risk, 60
Access rules, 79
Acquisition of hardware, 24–26
availability, 25
criticality, 25
disposal, 25
hardware components, 25
implementation, 25
operation and maintenance, 25
phases, 24–25
planning, 25
reliability, 25
selection criteria, 25
Adverse opinion, 88–89
Alternative site procedure, 128
Analytical procedures, 67, 74
audit evidence collection, 66
substantive tests, 80
use of, 76
Antivirus audit checklist, 218
Application control, 10–11
access control, 49
consistency, 72
input control, 10
output control, 11
processing control, 11
review, 188
Application control review,
188–190
access log review, 189
log-on attempts, 189
module interfacing, 189
password management, 189
user ID maintenance, 189
user profile maintenance, 188
virus detection and protection, 189
Application development
checklist, 219
Application program, 83
analyzing, 83
Application software, 44–45
best practice controls, 44
database management systems, 47
transaction processing checklist, 275
Asset classification and control, 18, 223
checklist, 223
hardware inventory register, 18, 140
Asset safeguarding, 64–65
  objectives, 64
  procedures, 64
Attack, 61
  cyberattack, 160, 162
  vulnerable to attack, 162
Audit area selection, 74
Audit checklist. See ISecGrade checklist
Audit documentation, 86
Audit evidence, 66–69, 156
  analytical procedures, 67, 74
  audit trail, 13, 46, 52, 67–70, 79
  categories of evidence, 66
  confirmation, 66
  documentation, 66, 86, 87, 149
  inquiry, 66
  logs, 53, 67, 69
  observation, 66, 81
  physical examination, 66
  processing accuracy, 66
  screenshots, 66
  software testing results, 67
  technique of collection, 66
Auditing approaches, 89–91
  auditing around the computer, 89
  auditing through the computer, 91
  auditing with the computer, 90
Audit objectives, 62, 91
Audit plan, 72–75
  audit area selection, 74
  background overview, 74
  checklist, 210
  competency, 75
  developing an audit plan, 76
  engagement letter, 73
  materiality level, 74
  scoring, 75
  simulation and modelling, 75
Audit procedure, 75–77
  analytical review procedures, 76
  audit plan, 76
  background information, 75
  compliance tests, 76
  evaluation, 77
  opinion, 77
  substantive tests, 77
  summary of evidences, 77
  understanding of controls, 77
Audit program, 71
  audit checklist, 71
  computerized audit program, 83
  consistency, 72
  resources planning, 72
  selection reference, 204
Audit prioritization, 103
Audit questionnaire, 85
  administering the questionnaire, 85
  characteristic of user, 85
  layout and structure, 86
  nature of information, 85
Audit report, 87
Audit risks, 108–111
  assessment, 109
  combined risk assessment, 109, 110
  control risk, 110
  detection risk, 109, 110
  inherent risk, 110
Audit steps, 75–77, 91–92
Audit team assignment, 92
Audit tools and techniques, 81–84
  base case system evaluation, 81
  control flowcharting, 83
  customized audit program, 82
  embedded audit data collection, 82, 91
  extended records, 82
  generalized audit software, 82
  integrated test facility, 81
  mapping, 83, 188
  parallel simulation, 81
  query language software, 84
  snapshots, 83
  terminal audit software, 82
  test data method, 81
  tracing, 31, 69, 83
  transaction selection, 82
  utility programs, 44, 49, 83
Audit trail, 13, 46, 52, 67–70, 79
  access rules, 79
  control grids, 66, 79
  control totals, 79
  document number, 79
  error logs, 69, 70
  exception and statistical reports, 70
  run-to-run control totals, 70
  system logs, 69, 70, 180, 194
  transaction logs, 69, 79
Audit work planning memo, 91
  activities and deliverables, 92
  audit objectives and scope, 62, 91
  audit process, 91
  audit team assignment, 92
  testing techniques, 92
Audit working papers, 86
Audit work process flow, 93
Authentication, 34
  authentication for external connections, 34
  node authentication, 34
  user authentication, 34, 49, 175
Authentication devices, 24
  biometrics, 24
  checklist, 223
  smart cards, 24
Authorization, 12
  organizational and operational control, 10
Automated matching, 50
Availability, 8, 62
  hardware availability, 28
  network availability, 39
Backup, 12
  business resumption plan, 123–126
  firewall operation, 191, 192
  information backup, 52
  location, 120
  media, 120
  recovery controls, 12
  recovery procedures testing, 126
  requirement, 120
  review, 185
  testing, 191
Back-up plan, 121
  disaster recovery plan checklist, 234
  plan maintenance, 126–127
Base case system evaluation, 81
Batch total, 50
Binary format, 128
Biometrics, 24
Black box, 89
Business continuity, 115–145
  business impact analysis, 116
  checklist, 234
  controls, 10
  forms and documents. See Business continuity forms
  plan maintenance, 126
  plans. See Business continuity plan
  recovery procedures, 126
  strategy, 122
  vital records retention, 127
Business continuity forms, 128–145
  alternative site, 128
  communication resources, 31, 130
  contingency log, 131
  contingency plan contact information, 132
  documentation list, 135
  emergency procedures, 136
  external support agreements, 139
  hardware inventory, 140
  information asset usage procedures, 141
  layout inventory, 142
  software inventory, 143
  team staffing and tasks, 144
  vendor contact list, 145
Business continuity plan, 116, 126
  disaster recovery plan, 116, 119
  emergency preparedness, 121
  incidence response plan, 116, 118
  resumption plan, 123–126
Business continuity strategies, 122
  prevention, 122
  recovery, 123
  response, 122
  restoration, 123
  resumption, 122
Business disruption risk, 60
Business impact analysis, 116
  contagion impact, 117
  process, 116
  requirement for recovery, 117
  service level agreement, 116
Business resumption 123–126
Business strategy checklist, 224
Cabling security, 20
Centralized processing, 187
Chain of custody, 171
Change control, 39, 56
Change management, 56, 190
  checklist, 225
  database, 190
  hardware, 30–31, 182
  network and communication, 183
  software, 183
Check digit, 51
Client-server architecture, 23
  checklist, 229
Cloud computing, 9, 43
Code comparison, 31
  source code comparison
  software, 31
Cold site, 295
Combined risk assessment, 109, 110
Communication resources, 31, 130
Communication software, 46, 183
  checklist, 230
Competency center, 75
Completeness control, 50
Compliance review, 76, 77–78
  audit trails, 78
  overall tests, 78
  test of controls, 77
  test of transaction, 78
Computer forensics, 168
Computer program, 43
Concurrency control, 47
Confidentiality, 15, 23, 38, 44, 62
Confirmation, 66
Connection time
  limitation, 49
Consistency, 72
Contagion impact, 117
Contingency log, 131
Contingency plan, 185
  contact information, 132
  coordinator, 144
Control flowcharting, 83
Control grid, 66, 79
Control objectives, 61
Control risks, 74, 110
Control totals 79
  verification, 69
Corrective control, 11
Credit risk, 60
Criticality, 107
  hardware, 25
  impact analysis, 116
  sensitive system isolation, 50
Cryptography, 34
Customer service risk, 60
Customized audit program, 83
Cyberattack, 160
  denial of service, 162
  malware, 162
  phising, 162–165
  spyware, 162
  trojan, 162
  virus, 162
  worm, 163
Cybercrime, 160–161
Cyber forensics, 168–170
  computer forensics, 168
  network forensics, 168–170
  process, 168
Cybersecurity, 159
Cyberstalking, 161
Database administration, 189
  change management, 190
database logs, 190
encryption of data, 191
passwords, 190
privilege level, 190
problem management, 190
segregation of duties, 190
super-user accounts, 190
Data communication checklist, 231
Data integrity, 62, 75, 78, 80
Data integrity risk, 60
Data verification, 82
  customized audit software, 83
generalized audit software, 82
  terminal audit software, 82
Database administrator, 189
Database controls, 55
Database management system, 47
Daubert reliability test, 172
Demilitarized zone, 193
Denial of service, 162
Dependency check, 51
Destruction of assets, 63
Detection risk, 109, 110
Detective control, 11
Digital evidence, 170
  acceptability tests, 172
  chain of custody, 171
  examination environment, 171
  manner of gathering, 171
  ownership and licensing, 171
  presenting digital evidence, 170
  technical analysis, 171
  technical capability, 172
  technical tools, 171
  techniques and methodology, 171
Digital signature, 128, 160
Digitizing, 128
Directive control, 11
Disaster, 119
Disaster recovery, 115
Disaster recovery plan, 116, 119–121
  backup plan, 121
checklist, 234
emergency plan, 120
recovery plan, 121
test plan, 121
Disclaimer, 88
Disk image, 170
Disposal, 26
  equipment, 28
e-waste, 27
Disruption, 20, 60, 63
Documentation, 66, 86, 87, 149
  procedure manual, 14
  user documentation, 25
Documentation list, 135
Document control, 10
  movement of documents, 13
Document flow, 77
Document number, 79
Document reconciliation, 51
Document review, 80
Domain name server, 193
Downtime, 25, 151
Downtime credit, 126
E-commerce audit, 147–158
  accounting and processing, 152
  administration, 151
  general overview, 149
  impact on internal control, 155
  implementation, 151
Internet security
  administration, 153
  legal and regulatory matters, 153
  objectives, 148
  policies and procedures review, 155
  policies and procedures, 151
  preliminary review, 150
E-commerce
  audit evidence, 156
  impact on internal controls, 155
  international laws, 156
  process alignment, 156
  security, 155
  transaction integrity, 155
Effectiveness, 62, 63
Efficiency, 63
Electronic fund transfer checklist, 237
Embedded audit data collection, 82, 91
Emergency plan, 120, 121
preparedness 121
procedure, 136
Emergency procedure, 136
Encryption, 32
Encryption of data, 191
storage level, 191
VPN level, 191
Enforced path, 33
Engagement letter, 73
Entropy, 15
Equipment life-cycle planning, 27
key variables, 28
Error log, 69, 79
Ethical hacking, 166
Evidence
analytical procedures, 67, 74
audit trail, 67–70, 79
categories of evidence, 66
collection and evaluation, 65
confirmation, 66
cyberforensics, 168–170
digital evidence, 170
documentation, 66
evaluation, 77
impact of e-commerce, 156
inquiry, 66
logs, 67, 69
observation, 66, 81
physical examination, 66
presenting digital evidence, 170
processing accuracy, 66
screenshots, 66
software testing results, 67
technique of collection, 66
E-waste, 27
Exception and statistical reports, 79
Existence check, 51
Expected value of loss, 65
Exposure, 61
Extended records, 82
External report misstatement risk, 60
External support agreement, 139
False positive, 172
Fault logging, 70, 149
File and directory protection checklist, 240
Financial report misstatement risk, 60
Firewall, 191, 192
Flowchart, 156–158
Forensics, 168
Format check, 51
Fraud risk, 60
Functionality, 28
Gateway, 36
General controls, 9–10
access, 10
business continuity, 10
data and procedural, 10
hardware and software, 10
organizational and operational, 10
system development and documentation, 10
Generalized audit software, 82
Goals of IS audit, 62
Hacking, 166
Hardware, 18
acquisition, 24–26
authentication devices, 24
availability, 28
change management, 30–31
client-server architecture, 23
disposal of equipment, 28
information system facilities, 22
integrity, 18
maintenance, 26–27
management of obsolescence, 27–28
network and communication, 31–40
peripheral devices and storage media, 22–24
problem management, 29–30
Hardware audit, 182, 201, 205
Hardware control, 10
Hardware inventory register, 18, 140
Hardware security, 17–40
  asset control and classification, 18, 223
  authentication for external connections, 34
cabling security, 20
enforced path, 33
management of peripheral devices, 22
management of removable computer media, 23
network availability, 39
network connection control, 36
network integrity, 38
network monitoring, 39
network routing control, 36
network services, 36
network usage policy, 32
node authentication, 34
objective, 17
physical access and service disruption, 20
physical equipment placement and protection, 19
power supplies, 19
protection during transmission, 39
segregation of networks, 35
wireless network, 40
Hash total, 69, 79
Hash value, 169
Help desk, 194
Human resources, job definition, resourcing and training
  checklist, 242
Identification tokens, 35
Impact analysis, 116
Implementation, 25
e-commerce, 151
packaged software, 257
postimplementation, 55
preimplementation, 54
security policy, 243
Implementation of IS security policy checklist, 243
Incident response plan, 116, 118–119
definite indicators, 119
possible indicators, 118
predefined situations, 119
probable indicators, 119
Information assets, 8–9
types of assets, 162
usage procedure, 141
Information backup, 52
Information harvesting, 50
Information systems audit, 3
  asset safeguarding, 64–65
  auditing around the computer, 89
  auditing through the computer, 91
  auditing with the computer, 90
  checklists 197–279
  conducting, 71–100
  coverage, 15
documentation, 86–89
legal requirements, 4–7
objectives, 62
procedures and approaches, 75–77
requirements, 59–70
system effectiveness, 63
system efficiency, 63
system environment, 7
tools and techniques, 81–84
Information systems auditor, 4
Information systems audit plan, 72–75
  checklist, 210
See also Audit plan
Information systems facilities, 22
  alternative site, 129
Information systems security policy checklist, 245
Inherent business risk, 73, 105, 110
Input controls, 10
Input output device management, 42
Inputs, 12
Input validation, 155
Inquiry, 66
Inspection, 66, 80
Installation
   control issues, 53
Insurance, 56, 72, 182
Integrated test facility, 81
Integrity, 3, 62, 75, 88
   data integrity risk, 60
   digital signature, 128, 160
   hardware, 18
   network, 38
   security threat, 161
   software, 42
   transaction integrity, 155
Internet banking, 155, 161, 176, 189
Internet connection, 191
Internet protocol, 35
Internet security, 153
   checklists, 209
   client server, 229
communication
   software/devices, 230
   data communication (router), 231
   disaster recovery plan, 234
   domains, 200
   electronic funds transfer, 237
   emergency preparedness, 121
   file and directory protection, 240
   format of audit report, 206
   grading audit report, 202
   human resources, job definition,
      resourcing, and training, 242
   implementation of information
   systems security policy, 243
   information system
      security policy, 245
   Internet security, 244
   legal compliance, 249
   local area network, 247
   long-term information technology
      strategy, 251
   maintenance questionnaire, 253
   management control system, 254
   methodology, 200
   operating system, 256
packaged software
   implementation, 257
   parameter setting, 258
   peripheral devices and storage
      media, 259
   physical access control, 260
   physical environment, 262
   problem management, 265
   security management, 266
   segregation of duties, 268
   selection of checklist, 203
   short-range information technology
      plan, 269
   software license, 270
   system conversion and
      reconciliation, 271
<table>
<thead>
<tr>
<th>System Software Control</th>
<th>Wireless Network</th>
<th>Legal Risk</th>
<th>Licensing Issues</th>
<th>Linking of Accounts</th>
<th>Local Area Network Checklist</th>
<th>Long-Term IT Strategy Checklist</th>
<th>Maintenance</th>
<th>Malicious Software</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>271</td>
<td>278</td>
<td>60</td>
<td>171, 200</td>
<td>188</td>
<td>247</td>
<td>251</td>
<td>25, 26–27</td>
<td>52</td>
<td>162</td>
</tr>
<tr>
<td>Third-Party and Vendor Services Review</td>
<td>275</td>
<td>4–7</td>
<td>55</td>
<td>188</td>
<td></td>
<td></td>
<td>253</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Processing</td>
<td>Utility Program</td>
<td>Securities and Exchange Commission</td>
<td>Statement on Auditing Standards</td>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>277</td>
<td>277</td>
<td>4</td>
<td>5</td>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Security Policy Checklist</td>
<td>IT Fixed Asset Register</td>
<td>Sarbanes-Oxley Act</td>
<td>Legal Compliance Checklist</td>
<td>245</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Security Policy Checklist</td>
<td>IT Fixed Asset Register</td>
<td>Legal Requirement</td>
<td>Legal Compliance Checklist</td>
<td>249</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Security Policy Checklist</td>
<td>IT Fixed Asset Register</td>
<td>Legal Requirement</td>
<td>Legal Requirement</td>
<td>4–7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Management Control System | Mapping | Materiality Level | Mathematical Accuracy | Matrix | Control Grid | Risk | Mean Time Between Failures | Memory Management | Memory Resident Program | Migration Control | Modem | Modification | Module Interfacing | Monitoring | Continuous | Monitoring of Data Processing Transactions | Monitoring of Network | Node Authentication | Encryption | Enforced Path | Equipment | Forensics | Identification Token | Integrity | Intrusion Detection | Intrusion Prevention | IP Address | Local Area Network | Monitoring | Node Authentication |
|---------------------------|---------|------------------|-----------------------|--------|--------------|------|---------------------------|------------------|------------------------|-----------------|-------|--------------|-------------------|------------|-------------|-----------------------------|------------------|------------------|-----------|-------------|------------------|----------|-----------------|-----------------|-----------|-------------------|-------------|-------------------|
| 254                       | 83, 188 | 74               | 51                    | 75     | 79           | 103, 105, 111 | 25                       | 42              | 44                     | 186             | 22, 191 | 63           | 189                | 14, 76      | 76           | 82                         | 39               | 34               | 32         | 33           | 38               | 168       | 35             | 35              | 35         | 247               | 39       | 34               |

<table>
<thead>
<tr>
<th>Network</th>
<th>Multiple Feed</th>
<th>Multisite Audit Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>19</td>
<td>111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Access Control</th>
<th>Address Translation (NAT)</th>
<th>Audit</th>
<th>Availability</th>
<th>Change Control</th>
<th>Connection Control</th>
<th>Demilitarized</th>
<th>Domain Name Server</th>
<th>Encryption</th>
<th>Enforced Path</th>
<th>Equipment</th>
<th>Forensics</th>
<th>Identification Token</th>
<th>Integrity</th>
<th>Intrusion Detection</th>
<th>Intrusion Prevention</th>
<th>IP Address</th>
<th>Local Area Network</th>
<th>Monitoring</th>
<th>Node Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>193</td>
<td>183</td>
<td>39</td>
<td>36</td>
<td>193</td>
<td>193</td>
<td>32</td>
<td>33</td>
<td>38</td>
<td>168</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>247</td>
<td>39</td>
<td>34</td>
</tr>
</tbody>
</table>
Network (continued)
path, 33
policy on use, 32
port, 33
proxy, 193
routers, 47, 192
routing control, 36
secure connection, 32
security of services, 36
segregation, 35
session, 38
switching, 47
usage policy, 32
user authentication, 34, 49, 175
virtual private, 192
wireless audit checklist, 40, 278
Node authentication, 34
Nonrepudiation, 160
Nonstatistical sample selection
   method, 84

Objectives of IS audit, 62
Observation, 66, 81
Obsolescence, 27–28
Operating software, 42
Operating system, 42, 98
   access control, 48
   checklist, 256
   logs, 194
Operation and maintenance, 25
Operational control, 10, 50
   completeness control, 50
   programmed edit checks, 51
Operator’s log, 70
Opinion of auditor, 73, 77
   adverse, 88
   disclaimer, 88, 89
   qualified, 88, 89
   unqualified, 88, 89
Output, 11, 13, 157
   device management, 42
Output control, 11
Overall tests, 78

Packaged software implementation, 257
Parallel simulation, 81
Parameter setting, 258
Password, 158
   maintenance, 184
   management system, 48, 175, 189
   router password management, 192
   secrecy, 184
   usage, 190
Path, 33
Penetration testing, 166
Performance level, 28
Peripheral devices, 22–24
   checklist, 259
Per server license, 55
Phishing, 162–165
Physical access, 20
   control checklist, 260
   service disruption, 20
Physical environment, 181
   checklist, 262
Physical equipment placement, 19
Physical examination, 66
Physical harm risk, 60
Plan maintenance, 126
Planning, 200
   audit work memo, 91
   business continuity, 122
   information system, 74
   life cycle, 28
   resource, 72
Policy
   information systems security, 245
   use of network, 32
   user registration, 174
Port, 33
   restriction, 191
Postimplementation issues, 55
Power supplies, 19
Preimplementation issues, 54
Prerecorded input, 52
Prevention strategy, 122
Preventive control, 11
Prior data matching, 51  
Privacy violation, 63  
Privileges, 46, 48  
  level, 190  
  management, 48  
Probability assignment, 64–65  
Problem management, 29, 190  
  checklist, 265  
Procedural control, 10, 254  
Procedure manual, 14  
Processing accuracy, 66  
Processing control, 11  
Process management, 42  
Production environment, 30  
Profiling of risk, 60  
  access risk, 60  
  business disruption risk, 60  
  credit risk, 60  
  customer service risk, 60  
  data integrity risk, 60  
  financial report misstatement risk, 60  
  fraud risk, 60  
  legal and regulatory risk, 60  
  physical harm risk, 60  
Programmed edit check, 51  
  audit trail, 52  
  check digit verification, 51  
  dependency check, 51  
  document reconciliation, 51  
  exception reports, 52  
  existence check, 51  
  format check, 51  
  mathematical accuracy check, 51  
  prerecorded input, 52  
  prior data matching, 51  
  range check, 51  
  reasonableness check, 51  
Programming and technical skill set, 28  
Proxy, 193  
  
Qualified opinion, 88, 89  
Quality assurance function, 220  
Quality control, 11, 62  
Query language software, 84  
Questionnaire. See ISecGrade checklist  
Random sampling, 84  
Range checks, 51  
Read-only memory, 43  
Reasonableness check, 51  
  checklist, 271  
Record retention, 127  
Recovering deleted data, 170  
Recovery  
  checklist, 234  
  control, 12  
  plan, 119–121  
  procedures testing, 126  
  requirement, 117  
  strategy, 123  
  time objective, 118  
Regulatory risk, 60  
Reliability, 25  
  Daubert test, 172  
Removable computer media, 23  
Repair and maintenance, 184  
Reperformance, 80  
Report  
  audit, 87, 206  
  day-end, 185  
  draft, 93  
  exception, 52, 186  
  final, 93  
  statistical, 79  
  summary-level report, 195  
Reporting, 103  
  hardware audit, 182  
  ISecGrade format, 206–207  
  password maintenance, 184  
  software audit, 183  
Representation, 108  
Resource planning, 72  
Response strategy, 122  
Response time credit, 26  
Restoration strategy, 123
Resumption strategy, 122
Retention, 127
Risk, 60
    access, 60
    analysis, 59
    assessment, 76, 104
    attack, 61
    audit risk, 73, 108–111
    business disruption, 60
    combined risk assessment, 109, 110
    control risk, 74, 110
    credit, 60
    customer service, 60
    data integrity, 60
    exposure, 61
    financial report misstatement, 60
    fraud, 60
    inherent risk, 73
    legal and regulatory, 60
    likelihood, 61
    matrix, 105
    physical harm, 60
    threat, 61
    vulnerability, 61
Risk-based information systems audit,
    101–113
    assessment, 102
    audit process, 109
    audit risk, 73, 108–111
    conducting, 101–103
    control risk, 74, 105, 110
    inherent business risk, 73, 105
    management strategy, 112
    matrix, 105
    prioritization, 102
    profiling, 102
    reporting, 103
    sample determination, 107
    sample selection, 108
Routers, 47, 192
    checklist, 231
    password management, 192
Run-to-run total, 79
Safeguarding, 64
Sample selection, 84, 108
    determination, 107
    nonstatistical, 84
    statistical, 84
    stratified, 84
Sample size, 107–108
    investment, 108
    mission criticality, 107
    representation, 108
Sampling techniques.
    See Sample selection
Scoring, 75
Screenshots, 66
Secure connection, 32
Security control,
    information system security policy, 243
    network and communication
        issues, 31
    segregation of networks, 35
Security management, 182
    checklist, 266
Security threat, 161
    threat
        types, 162–163
Segregation of duties, 14, 190
    checklist, 268
Segregation of networks, 35
Sensitive system isolation, 50
Service disruption, 20
Service level agreement, 117
Session, 38
Short-range information technology
    plan, 269
Simulation and modeling, 75
Site license, 55
Slack, 169
Smart cards, 24
Snapshot, 83
Software
    audit, 182
    change management, 225
    integrity, 42
inventory, 143
license checklist, 270
licensing, 65
packaged software
implementation, 257
query language, 84
security issues, 41–57
system software controls, 271
testing, 67
utility software checklist, 277
Software for audit, 82–83
customized, 83
generalized, 82
terminal, 82
Software access control, 211–217
Software control, 10
operating software, 42
packaged software, 257
system software, 271
utility software, 277
Software inventory, 143
Software license checklist, 270
Source code, 31, 161
Source documents, 79
Spam mail, 161
Spoofing, 97
Spyware, 162
Statistical sampling, 84
Storage,
checklist, 259
damage to media, 111
enCRYption of data, 191
information, 13
internal, 157
media, 22
recovering deleted data, 170
Stratified sampling, 84
Structured query language (SQL), 184, 190
Substantive reviews and testing, 51, 77, 80
confirmation, 80
document review, 80
inspection, 80
reconciliation, 80
reperformance, 80
Super user, 190
Switches, 47
System conversion and reconciliation, 271
System development and
documentation control, 10
System development life cycle, 72, 219
System file management, 42
System log, 69, 180, 194
System parameters, 258
System software, 10, 41–42
checklist, 271
System understanding and review, 77
System utilities, 49, 177
Team staffing and tasks, 144
Techniques of evidence collection, 66
Terminal
audit software, 82
log on, 49
time out, 49
unattended, 186
Test
acceptability, 172
application program control, 81
backup and periodic recovery, 191
compliance, 76
cpyontrols, 77
Daubert, 172
integrated facility, 81
overall, 78
pack, 80
substantive, 77, 80
transactions, 78
Test of controls, 76, 77
Test data method, 81
Testing software, 67
Test plan, 121
Theft
assets, 63
identity, 175, 251
source code, 161
Thin client, 42, 43
Third-party vendor, 27
checklist, 273
Threat, 61
Tracing, 31, 69, 83
Transaction
initiation, 12
integrity, 155
log, 69, 79
processing checklist, 275
proxy, 187
selection, 82
system generated, 187
user generated, 187
walkthrough, 15, 83
Trojan, 162
Two-tier architecture, 23
Types of vulnerabilities, 166
infrastructure based, 166
practice based, 166
Unauthorized
access, 10, 33, 178
change, 30
programs and folders, 184
sign-on attempts, 176
use of network equipment, 38
use of unattended terminals, 176
Uninterruptible power supply (UPS), 19
Unqualified opinion, 89
Update, 167
Usage procedure, 141
User
access management, 48, 174
authentication, 34, 49, 175
ID maintenance, 189
output control, 11
password management, 48
profile management, 188
Utility programs, 44, 49, 83
checklist, 277
Validation, 51, 91, 155
Vendor
checklist, 273
contact, 145
contract, 154
outsourced, 15, 27
service review, 273
Virtual memory, 43
Virtual private network, 192
Virus, 155, 162
antivirus, 218
detection and prevention, 189
memory resident program, 44
protection against malicious software, 52
Vital record maintenance and retention, 127
Volume, 82, 102, 180
Vulnerability, 61
analysis, 165, 167
infrastructure based, 166
practice based, 166
Walkthrough, 15, 83
Wide area network, 95
Wireless network, 183, 202
checklist, 278
considerations, 40
Worm, 163