Index

AAA, 23
Accountability of Tax Dollars Act of 2002, 277
Accountable, 90–91, 114–115, 138–139, 157–158, 223, 251, 265, 292. *See also* RACI
Active management, 39–42, 76, 135, 147–148, 156–158, 160, 163
Affirmation, 80, 163
AICPA, 23
Aircraft Accident Report, 102, 127
American Accounting Association. *See* AAA
American Express, 49–50, 52, 203, 223
  authorizer's assistant, 51–52
  charge authorization request process, 50, 52
  travel related services (TRS), 49
American Institute of Certified Public Accountants. *See* AICPA
American Productivity and Quality Center. *See* APQC
Annual review of aircraft accident data, 105, 127
Anticipation, 101, 123, 127, 163
APQC, 61–62, 71, 92–93, 133
Arthur Andersen, 11, 61–62, 82, 251
Audit (ing), 32, 47, 83, 92, 179, 194, 200, 218, 277–278, 280–281, 289–291
  independent, 251, 256, 264
  internal, 7, 13, 23, 66, 85, 142, 149, 240, 243, 251–253, 257–258, 262–265, 267, 280, 291–293, 298
  external, 25–27, 240, 251, 253, 258, 261–264, 266, 276
Audit committee, 45, 87, 248, 251–252, 256–258, 286

Barings (Bank), 4–8, 11, 17, 19, 222, 285–287, 290, 296
Basel Accord, 24, 288
Basel Committee (on Banking Supervision), 10, 15, 21, 23–24, 34, 39, 47
Basel II, 24, 29–30, 33–34, 41, 44, 46, 292
Belgium, 24, 196
Blue Grass Airport in Lexington, Kentucky, 102–103
Board of Banking Supervision (England), 6, 15
Board of directors, 6, 39, 45, 86, 195, 245, 250–251, 256–257, 259–262, 264, 266–267, 269, 286, 297
Bouton, Daniel, 286, 289–290, 297
BPI, 53, 60, 64–65, 70
BPM, 49, 52–53, 55–56, 64–71, 76, 78–79, 161–165, 178, 193–194, 236, 238, 242, 244, 276, 281, 294, 296
BPMI.org, 67
BPMN, 67
BPR, 53, 60–61, 64–65, 70
BPTrends, 52–53
Brown, Bruce, 246, 270

Bush, George W., 25, 146, 251
Business continuity, 38, 192, 203, 205
Business goals, 65, 69, 70, 76, 79, 81, 85, 92, 99, 132, 161–162, 180–182, 186, 213, 224. *See also* Business objectives
Business objectives, 44, 81, 101, 133, 181, 224
  setting of, 85
Business practice, 25, 38, 149, 165, 204, 207, 239, 242
Business process (es), 12–15, 28–31, 79, 85, 92, 148, 174, 178, 182–183, 186, 192, 195, 243, 293
  design, 61, 106, 121
  designing or redesigning, 92, 161–162
  framework, 75
  handbook (*see* MIT)
  improvement (*see* BPI)
  integrated with operational risk (*see* integrated framework)
  management, 14–15, 44, 46, 49, 65, 67, 76–78, 92, 99, 101–102, 114, 122, 126, 160–163, 178, 181, 194, 219, 236, 238, 240–242, 265, 268, 276, 294 (*see also* BPM)
  management cycle, 65
  management notation (*see* BPMN)
  model (s), 63, 68, 76, 99, 106–107, 120–121, 124–126, 132, 162, 164
  monitoring, 41, 127, 129–142, 161–163, 194 (*see also* monitoring)
  objectives, 181
  offshoring (*see* offshoring)
  outsourcing (*see* outsourcing)
  redesign, 53, 60, 64, 71, 92, 125 (*see also* BPR)
  reviews, 97
  reengineering, 52, 53, 60 (*see also* BPR)
  simulate (ing/ion), 43, 67, 106–107, 113–114, 118, 161, 178, 193
Business Roundtable, 255–271

Canada, 24, 130–131, 144, 171–172, 195–196
Capability maturity model, 179, 204, 210. *See also* CMM
Capacity management, 186, 188, 190–191
CFO, 235. 249–251, 253, 269, 277–278, 291
CFTC, 279
Chain of command, 253–255, 263
Champy, James, 60
Cheney, Dick, 146, 160
Chief financial officer. *See* CFO
Chief Financial Officers Act of 1990, 277
Chief risk officer, 88–89, 91–92, 114–115, 138–139, 156, 158, 231, 234, 265–267, 269, 280, 282, 291. *See also* CRO
CMM, 179, 204, 210. *See also* Capability maturity model
COBIT, 31–32, 179–186, 192, 195–196, 213, 216, 218, 294
Code of ethics. *See* Ethics
Combined code on corporate governance, 257–258, 271
  Higgs report, 257
  Smith guidance, 257
  Turnbull guidance, 257–263, 271, 294
Committee of Sponsoring Organizations. *See* COSO
Commodity Futures Trading Commission. *See* CFTC
Commonly used operational risk framework, 40–42, 46
Communicate:
  deficiencies (*see* control deficiencies)
  results, 87–91, 112–115, 135–139, 148, 155, 158
  risks, 91–92, 156
Company-level controls, 27–29, 276, 294
Compliance, 13, 26, 193, 196, 200–201, 213, 217, 255–256, 267, 269
  department, 142, 287–288
  officer (s), 149, 280
  Noncompliance, 35–36
  with law (s), 29, 147, 182–183
  with regulation (s), 33, 183, 265
Comprehensive, 161, 163
  assessment, 150
  framework, 45, 161, 165
  guidelines, 174
  program, 40, 268
Configuration management, 188
Confirmation, 145, 163, 209
Consult, 90–91, 114–115, 138–139, 157–158, 223, 265. *See also* RACI
Consulting firm (*or* consultant), 21, 61, 290, 294–295, 298
Continuous process improvement. *See* CPI
Contract (s), 94–96, 98, 100, 107–111, 182–183, 199, 202, 204, 206–210, 212–216, 247, 295
Contractor (s), 123–124, 146
Control (s):
  activities, 30, 40, 184–185, 257
  areas, 13, 293
  business, 67
  company-level (*see* company-level controls)
  deficiency (ies) (*see* control deficiencies)
  documented, 12, 293
  documents, 88

failure (s), 44, 115, 129, 135, 138, 158, 163, 194, 235, 237, 257, 265, 285
framework, 32–33, 36, 134, 186
function, 13, 268
internal, 23, 25–28, 33, 180, 257–258, 260, 276–278
IT (*see* IT control)
objectives, 31, 87–88, 91, 180–181, 184–186, 192, 215
principles, 29
procedures, 7–8, 12
process (es), 145, 223, 259
risk management and control (*see* risk *or* operational risk)
system (s), 23, 41, 85, 106, 134
technology (*see* IT control)
Control deficiencies:
identify, 44, 76, 112, 115, 127, 129, 138, 142–143, 148–149, 157–158, 163–164, 228, 235–237, 244, 265, 285
actual / existing, 129, 240–242
classification, 38
measure, 136, 150–152, 282
mitigate, 127, 134, 153, 244, 277, 289
monitor, 131, 138
potential, 113, 115, 129, 149, 164, 236, 240, 265
report, 78, 244, 281
validation, 145
Control Objectives for Information and related Technologies. *See* COBIT
Cooper, Cynthia, 252–253, 270
Corporate culture, 33–34, 45, 88–89, 275, 282–283, 295. *See also* Culture
changing, 275
Corporate evolution, 33
Corporate governance, 13, 88, 245–270
code (*see* combined code on corporate governance)
improve, 182
model/structure, 165, 248
principles (of), 255–256, 259–260
role of, 245
statement on, 255
Corporation, 7, 33–37, 45, 59, 78, 85, 90, 129–131, 162–163, 165, 219, 229, 245–249, 255–256, 260–261, 270, 277–278, 292
history of, 246, 270
COSO, 23, 26–31, 34, 39, 41, 44, 46, 134, 140–142, 178, 257–258, 276, 294
principles, 29 (*see also* ERM)
Cost-benefit analysis. *See* Score
CPI, 53, 60, 70
Credit risk, 11, 20–21, 24, 28, 39, 288–289, 295
Credo, 84, 100
Crime of the century, 4, 286
CRM, 53, 63, 70
CRO, 138, 156–157, 231, 234–238, 243–244
Culture, 32–34, 79, 88–89, 163, 201, 226, 258, 270, 275–276, 278–284, 289, 291, 294
company, 79, 88, 163
corporate (*see* corporate culture)
(of) organization (s), 32, 226, 275, 280–282
Customer relationship management. *See* CRM

Dartmouth College, 247, 270
Davenport, Tom, 60
Decompose, 61, 63, 67, 106, 126
Defense, Department of, 146
Deficiency. *See* Control deficiencies
Dellarocas, Chrysanthos, 120–122, 124–125, 127
Design effectiveness, 27, 276. *See also* Operating effectiveness
Disaster recovery. *See* Business continuity
Disclosure, 29–30, 39–40, 42, 215, 259, 264, 277
DMAIC, 59. *See also* Six Sigma
Dresser Industries, 146
Drucker, Peter, 56

East India Company, 247
Ebbers, Bernie, 248
Edison, Thomas, 70
Effectiveness of internal controls, 27–28, 257–258, 276–277. *See also* Design effectiveness
Electric power:
company, 173
distribution, 170
generation, 170–171, 173
outage, 171
plant (s), 82, 170
transmission, 170–174
Encrypting, 131
End-to-end, 149. *See also* Front-to-back
Enhanced telecom operations map framework. *See* eTOM
Enron, 4, 11, 25, 61, 82–83, 100, 252, 256, 261, 296
Enterprise resource planning. *See* ERP
Enterprise risk management. *See* ERM
Environment, 32, 40, 129, 176, 180, 190, 194, 226. *See also* Risk environment
business (process), 52, 76, 87, 163
controlled, 227

Environment (*continued*)
external, 61, 224, 226
internal, 29, 224, 226
risk, (*see* risk environment)
setting, (*see* risk environment)
test, 230
update (*see* risk environment)
Environmental indicators, 136, 139, 237
ERM, 29–30, 39, 294
ERP, 53, 63–64, 70, 93
Ethics, code of, 82, 84, 100, 264
eTOM, 63
Exception handling, 122–124, 159, 264. *See also* MIT process handbook
Exception taxonomy. *See* Taxonomy
Executive committee, 81, 86–87, 90–91, 115, 139, 158, 265
Exxon, 3, 19, 20, 46, 296
Exxon Valdez, 17–19, 46, 222

FAA, 103–105
Failure
people, 225–31, 223, 234, 243
process (es), 17, 101–102, 112–113, 148–149, 157, 159–160, 226, 228, 243
system (s), 37–38, 149, 170, 175, 228, 243–244
technology, 174, 225 (*see also* failure, system)
FASB, 31
FDA, 84
Federal Aviation Administration. *See* FAA
Federal Reserve, 286–287, 290
FEI, 23
Feigenbaum, Armand, 58
Financial Accounting Standards Board. *See* FASB
Financial Executives International. *See* FEI
Fire marshal, 11–12, 14, 46, 231, 235, 243, 293–294, 296
Firefighter, 11–12, 46, 229, 235, 293
FirstEnergy (FE), 172
Food and Drug Administration. *See* FDA
Fortune 500, 198, 248
Fortune magazine, 52, 82
Framework:
BPM (see BPM)
business process (*see* business process framework)
business process management (*see* BPM *or* business process management)
COBIT (*see* COBIT)
control (*see* control)
COSO (*see* COSO)
ERM (*see* ERM)
integrated (*see* integrated framework)
operational risk (*see* operational risk framework)
operational risk management (*see* operational risk management framework *or* ORM framework)
ORM (*see* operational risk management framework *or* ORM framework)
PCF (*see* PCF)
process (*see* process)
process management (*see* process management)
risk (*see* risk)
risk control (*see* risk)
risk management (*see* risk)
SOX 404 (*see* SOX)
France, 24, 170, 173, 246, 286–287, 289–290
Franklin, Benjamin, 170
Fraud, 4–6, 25, 27–30, 52, 83, 149, 248, 251–252, 262, 277, 287, 289, 297
external, 10, 35, 175, 178
internal, 34–35, 175, 178
Front-to-back, 27–28, 36, 277. *See also* End-to-end

G10, 23
GAAP, 250
Galbraith, Jay, 231, 234
GAO, 277–278, 284
Gartner (Group), 52–53, 65, 193–194
Generally accepted accounting principles. *See* GAAP
Germany, 5, 24, 173, 246
Governance. *See* Corporate governance
Government Accountability Office. *See* GAO
Group of Ten countries. *See* G10
Guidance on monitoring internal control systems, 134, 142, 144. *See also* COSO

Halliburton, 146–147
Hamilton, Alexander, 248
Hammer, Michael, 60
Hand-off, 222, 224–227, 229–230
Health and Human Services, Department of, 221
Higgs report. *See* Combined code on corporate governance
Home Goods, 130
Hospital (s), 83, 187, 201, 220–223, 247
Houston Natural Gas, 82

IBM, 66, 291
ICCA, 200. *See also* Mattel
IDS, 66
IIA, 23
Incident management, 187–189
Inform, 90–91, 114–115, 138–139, 157–158, 223, 265. *See also* RACI
Information security. *See* Security
Information Systems Audit and Control Association. *See* ISACA
Information technology. *See* IT
Ingersoll-Rand, 146
Institute of Internal Auditors. *See* IIA
Integrated framework, 14, 47, 75, 78–79, 157, 162–165, 178, 180, 186, 193–195, 238, 268, 275, 281–283, 291, 293. *See also* ORM-BPM
Integrated model, 76, 162. *See also* Integrated framework
International Center for Corporate Accountability. See ICCA
International Herald Tribune, 146, 160, 297
International Organization for Standardization. *See* ISO
ISACA, 31, 179
ISO, 58, 59, 179, 195
IT Governance Institute, 31, 179, 182–185, 195–196, 209, 214, 216–218. *See also* ITGI
IT Infrastructure Library. *See* ITIL
IT:
  control (s), 28, 31, 119, 179, 186, 192, 253
  environment, 176
  goals, 180,–183, 186, 213
  governance, 179, 180, 195
  infrastructure, 63, 183, 185, 189–190
  management, 185–186, 267
  objectives, 181, 183 (*see also* IT goals)
  organization (s), 28, 174, 176–177, 232, 240
  process (es), 31, 140, 179–181, 183, 185–186
  resources, 180, 191
  risk, 32, 178, 181, 184–185
  service(s), 63, 175–178, 183, 185–188, 190–193, 202
  solution (s), 174, 180
Italy, 24, 172
ITGI, 31, 179, 195. *See also* IT Governance Institute
ITIL, 63, 179, 185–188, 190–192, 195, 294

Japan, 4, 24, 58
Johnson & Johnson, 83–84, 223
Johnson, Robert Wood, 83–84
Joint Commission on Accreditation of Healthcare Organizations and Affiliates, 222, 244

Kerviel, Jerome, 287–289
Key performance indicator (s). *See* KPI
Key risk indicator (s). *See* KRI
Klein, Mark, 120–122, 124–125, 127
Knowledge-based, 51, 120–122, 125, 127, 268
Knowledgespace, 61
Kotter, John P., 282, 284
KPI (s), 69, 132–134, 136–137, 139, 142, 157, 164
KRI (s), 136–137, 139, 142, 151, 164, 237
Kuhn, Thomas, 53, 71

Labor, Department of, 146–147
Lay, Ken, 82–83, 100, 252
LDDS, 248–249
Leeson, Nick, 5–8, 285–287
Life cycle, 53, 54, 65, 232
  BPM, 70
  operational risk and business process management, 85, 99, 160
  outsourcing, 209, 216
  IT service, 175
Long Distance Discount Services. *See* LDDS
Loss (es):
  events, 10, 12
  expected, 31, 283 (*see also* loss, potential)
  external, 22
  future, 12 (*see also* loss, potential)
  legal and liability, 35
  operational risk, 12, 22, 283
  people, 11, 13, 21–22, 49
  potential, 6, 21–22, 24, 28, 30–31
  process, 11, 13, 21–22, 36, 49
  risk of, 11, 13, 21, 49–50
  system, 11, 13–14, 21–22, 37, 49
  unexpected, 43 (*see also* loss, potential)
Luxembourg, 24

Market risk, 11, 20–222, 24, 28, 39, 287–289, 295
Marshalls, 130
Masking, 131
Mattel, 197–202, 296. *See also* ICCA
MCI, 4, 249. *See also* WorldCom
Metric (s), 52, 63, 127, 132, 148–149, 151, 180
  performance, 137, 140, 210
  qualitative, 143
  quantitative, 141–143
  risk, 44, 135–136, 139, 143, 151, 164, 237
  service level, 69

Microsoft:
operations framework, 174–175, 177, 196 (*see also* MOF)
Visio, 66, 116
Minow, Nell, 260–263, 265, 270–271
MIT
center for coordination science, 62
process handbook, 62, 121, 124, 126, 128, 159–160
Sloan School, 121
Model (s):
business, 64
function (al), 239–242
governance, 165, 259, 261, 263, 265–266
integrated, 76, 162 (*see also* integrated model)
model/simulate process, 15, 66, 76–78, 162, 193, 238
operating, 50
process, 53, 63, 65, 67–68, 70, 76, 97, 99, 106–107, 109–111, 116–121, 124–126, 132, 162, 164, 192
reference, 59, 61, 63, 70, 93, 100, 116, 133, 202, 218
Modeling, 66–67, 97, 99, 110, 116–117, 159, 161, 194
MOF, 174–175, 177–179 (*see also* Microsoft Operations Framework)
Monitor (ing), 30, 143, 148, 159, 164, 180, 189, 191, 194, 209, 213–214, 230–231, 242–243, 257–262
active, 41, 42, 228, 230, 294
business process (es), 65, 70, 127, 129, 134–136, 142, 161, 178, 282
continual/continuous, 26, 143
independent, 264
(and) manage supplier information, 93–94, 96, 98, 106, 108
ongoing, 39, 40, 76, 113, 132, 134–135, 161
operational risk, 120, 135, 245, 282 (*see also* monitor risk)
performance, 69, 85, 132, 135, 149, 215, 291
products, services and processes, 13, 293
(the) process (s), 15, 29, 44, 66, 68, 76–79, 112–113, 125, 129, 138, 155, 162–163, 228, 236, 238, 268
process monitoring, 61, 132, 157, 159
risk (s), 15, 43, 77–78, 134, 137–139, 141, 162, 223, 234, 237–238 (*see also* monitor operational risk)
risk action plan, 184–185
service delivery, 215–216
Monks, Robert, 260–263, 265, 270–271
Motorola, 59

National Commission on Fraudulent Financial Reporting, 23
National Transportation Safety Board, 19, 46, 102, 127. *See also* NTSB
Netherlands, 24
New Hampshire, 247
New York Stock Exchange, 23
New York Times, 4, 13, 100, 146, 217, 244, 296
Northern Natural Gas Company, 82
NTSB, 102, 105–106, 127

OECD, 259–261, 263, 271
Offshore (ing), 165, 197–198, 201–203, 205, 207, 209–211, 216–217, 234, 279
managing, 209
origins of, 202
risks of, 203, 206
role of, 197
Open standards benchmarking collaborative, 61
Operating effectiveness, 27, 277. *See also* Effectiveness of internal controls
Operational risk:
actual, 127
control (ling), 12, 245
disclosure of, 40
framework, 30, 40–42, 46, 147–148, 236, 275 (*see also* operational risk management framework)
history, 23–28
loss (*see* loss)
manage, 33–34, 42, 89, 165, 282
management, 28–29, 39, 41, 79, 99, 147–148, 158, 160, 163, 195, 219, 234–235, 290 (*see also* ORM)
management framework, 42–43, 77, 261 (*see also* ORM framework)
management group, 13
management organization (*see* ORM organization)
management process, 14, 212
management unit, 234
managing, 23, 32, 34, 39, 41–42, 46, 81, 88, 90, 147, 270, 275, 279–280, 283, 296
monitoring, 134–135, 137–139 (*see also* monitoring)
potential, 102, 106, 111, 127, 235
reporting of, 78
training, 280 (*see also* training)

principles of operational risk management, 39, 195
types of, 34, 38, 149
unit, 236, 239–240
Operationalize, 75, 79, 163, 165
Organization for Economic Cooperation and Development. *See* OECD
Organization (al), 34, 38, 40, 81, 89, 132–135, 138, 141, 149–152, 154–156, 159–160, 165, 202–210
activities/processes, 53, 60–61, 68, 93, 134, 142
(risk) appetite, 30, 84, 86, 113, 157
characteristics, 62
culture, 32, 275–276, 280–284 (*see also* corporate culture)
definition/description, 223–226
design principles, 231
goals/objectives, 29, 52, 62, 85, 87, 99, 224
governance, 254, 259–260, 263–266, 268, 293–294
history, 246–248 (*see also* corporation, history of)
impact, 42, 44
IT, 28, 174–177, 179, 181, 184, 187, 191, 225, 232
management, 32
performance, 30, 97
professional, 21
risk (s), 43, 113, 143, 149, 226, 234–237, 290, 293
role of, 219
structure, 62, 85, 245
technology (*see* IT)
tone, 29, 39, 278
ORM, 28, 33–34, 41, 44, 49, 83, 87, 92, 155, 169, 194, 223, 279, 282–283, 292, 296
activities, 42, 164, 244
approach, 59
culture, 278
definition of, 60
framework, 24, 28, 30, 39–30, 42, 45–46, 75–76, 79, 81, 86, 129, 134–135, 161, 236, 244
function, 238, 242, 281, 284, 293 (*see also* ORM organization *or* ORM unit)
implementation of, 89 (*see also* ORM, installing)
installing, 88, 292 (*see also* ORM, implementation of)
goal of, 26
organization, 223–235 (*see also* ORM function *or* ORM unit)
principles, 39, 99, 290
process, 138, 285
program, 40, 81, 89, 243, 295
structure, 75, 81, 86 (*see also* ORM framework)
unit, 236, 238 (*see also* ORM function *or* ORM organization)
ORM-BPM: *See also* ORM and BPM
framework (integrated), 78–79, 162–164 (*see also* integrated framework)
toolbox, 79
ORM and BPM, 163, 165, 193, 238, 242, 244, 294. *See also* ORM-BPM
Outsource (ing), 10, 12, 165, 197–198, 201–214, 216–217, 225, 234, 279, 293, 295
managing, 209
origins of, 202
risks of, 203, 206
role of, 197
Oxley, Michael, 25

Paradigm (s), 53–54, 58, 60, 64, 70
life cycle of, 53–55
Parker, Hugh, 260, 271
PCAOB, 25–28
PCI, 61, 92–96, 98
People failure. *See* Failure
Policies, 52, 119, 182–183, 213, 255, 257, 259, 292
and procedures, 22, 40, 42, 44–45, 86, 88–90, 101, 138, 216, 227–228, 282
corporate, 82–84
policies, procedures and control objectives, 87–88, 91, 164
policies, procedures and standards, 91, 237, 265
Potential risk
detect, 120
determine (ing), 15, 41, 43–44, 76–79, 101–102, 111, 113, 115, 129, 161–162, 223, 235–238, 242
identify (ing), 114, 120, 127, 137
indicated, 143
managing, 113
mitigate, 102, 127
predict, 294
reduce, 163
resolve, 120
PricewaterhouseCoopers, 289–290, 297. *See also* PwC
Principles of corporate governance. *See* OECD
Privacy commissioner of Canada, 131, 144
Proactive operational risk management (ORM) framework, 42–43, 45–46, 75, 161, 236, 243. *See also* ORM framework

Procedures, 51, 68, 97, 142, 151, 214, 221–222, 225–226, 229, 288–289
(and) controls, 7–8, 11–12, 20, 229–231, 243, 293
(and) policies, (*see* policies)
Process:
business. *See* Business process
classification framework. *See* PCF
failure. *See* Failure
handbook. *See* MIT
history, 53, 106, 150
modeling, 66. 67, 76, 99, 117
taxonomy. *See* Taxonomy
Processing
errors, 36–37, 149
financial, 28
technology, 140
transaction, 112, 152, 211, 265, 295
Public Company Accounting Oversight Board. *See* PCAOB
Public Company Accounting Reform and Investor Protection Act of 2002. *See* SOX
PwC, 290–291

Quality reports, 109–110

RACI, 89–91, 114–115, 126, 138–139, 157–158, 180–181, 215, 223, 236, 265. *See also* Responsible, Accountable, Consult, and Inform
RACIO. *See* RACI
RASCI. *See* RACI
Regulation, 35, 149, 199, 206, 217, 258, 276. *See also* Compliance
Rehearsal (s), 227–228, 230, 234
Remediation, 112, 115, 131, 148, 152, 158
Reputation, 11, 19, 21–22, 37–38, 86, 124, 131, 147, 149, 202, 248, 256
reputation (al) cost (s), 11, 145, 152
reputation (al) risk, 21–22, 152, 206, 295
Responsible (not pertaining to RACI), 7, 10, 12, 26, 32, 39, 86, 99, 156, 187, 189–190, 201, 220–221, 227, 236, 260, 263, 276–277, 287, 293, 295
Responsible (as part of RACI), 89–92, 114–115, 138–139, 157–158, 223, 265. *See also* RACI
Reynolds, Sir Joshua, 70
Risk:
accept, 158, 294
active risk management, 29–30, 40, 76, 156, 161 (*see also* active management)
appetite, 29–30, 40–41, 45, 79, 81, 86, 113, 149, 156–157, 219, 235, 291
assess, 181, 265
assessment, 29–30, 143, 184–185, 192, 212, 216, 279, 288, 291
business, 11, 21, 32, 181–182, 193, 213
control, 30, 33, 39, 176, 245
credit (*see* credit risk)
committee, 8, 87–92, 115, 138–139, 156, 158, 265, 267–269
environment (*see* risk environment)
framework, 75, 161 (*see also* operational risk)
IT (*see* IT risk)
key risk indicator (*see* KRI)
legal / liability, 11, 21, 35, 147
loss (*see* loss)
manage, 15, 32, 43–44, 77–78, 162, 169, 195, 208, 234, 236–238, 242, 281
management, 6, 17, 20, 24, 27, 29, 32–34, 38, 42–47, 280–282, 291, 295 (*see also* active risk management *or* operational risk)
management organization, 165, 234 (*see also* organization)
market (*see* market risk)
mitigate (ion), 34, 42, 45, 158, 181, 211, 208, 215, 237, 265
monitor (*see* monitor)
operational (*see* operational risk)
potential (*see* potential risk)
reputation (*see* reputation risk)
techniques, 28
technology (*see* IT risk)
unexpected, 20
unit responsibilities, 236
vision and principles, 86–87, 91, 164
Risk environment, 15, 39–43, 45, 76–78, 83, 86–87, 89–91, 113–114, 156, 161–162, 223, 227–228, 236–238, 258, 265–266
set/setting, 15, 29, 39–43, 45, 76–78, 83, 86–87, 89–91, 113, 156, 161–162, 164, 223, 227–228, 236, 238, 242, 265–266, 268
update/updating, 15, 42–43, 77–78, 83, 86–87, 89–91, 113, 115, 156, 158, 162, 236, 238
Risk objectives, 29–30, 81
setting, 86
Risk-based approach, 26–27, 88, 135, 138, 142
Roles and responsibilities, 19, 30, 42, 44, 101, 164–165, 215–216, 223–224, 226, 231, 265, 294
document (ing), 90–91, 237
set and update, 87, 89, 91

Roosevelt, Franklin D, 25, 55
Rowley, Coleen, 252

Sarbanes, Paul, 25
Sarbanes-Oxley Act of 2002, 25, 206, 249, 251, 256, 276. *See also* SOX
SCOR, 63, 70, 93, 100, 116, 132–133, 202
Score (s) / scoring, 112, 150–159, 237, 283, 294
  deficiency risk score, 154–156
  mitigation cost score, 153–156
Scorecard, 181, 213
SEC, 4, 23, 25–28, 31, 251, 257, 276–279, 292. *See also* Securities and Exchange Commission
Securities Act of 1933, 276
Securities and Exchange Commission, 23, 47, 251, 270, 276, 284, 292. *See also* SEC
Securities Exchange Act of 1934, 47, 270, 276
Security, 102, 144, 149, 177, 186, 198, 215
  application/data, 140, 165
  breach(es), 34, 36–37, 131
  information security, 37, 131, 265
  physical security, 36
  system/technology, 22, 152–153, 180, 191, 225
Sentinel events, 222, 244
Service level (s), 174, 176–177, 180, 183, 190–191, 203, 210, 212–213
  agreements, 69, 211
  management, 188, 190–191
  metric (s) (*see* SLM)
SFAS 5, 31
Shareholder (s), 11, 32, 45, 69, 84, 92, 240, 245–246, 248, 250–253, 256–260, 263, 289
  communication to/reporting to, 29, 263–264, 292
  protect, 259
  value, 12, 234, 256
Short, James, 60
Simulation, 68, 70, 91, 99, 101–102, 106, 126, 131, 159, 164, 173, 178, 237
  automated, 67 (*see also* simulation, system)
  of business processes, 43, 101, 106–107, 113–114, 118, 120 (*see also* simulation, process)
  of operational risk (s), 111–112
  people/rehearsal, 227–228, 230 (*see also* rehearsal)
  process, 44, 61, 76, 111, 115, 127, 162, 194, 294 (*see also* simulation of business processes)
  system (s), 114, 116–117, 119, 193 (*see also* simulation, automated)
Six Sigma, 59, 204, 294
Skilling, Jeffrey, 83, 100
SLM, 69
SMART, 140
Smith, Bill, 59
Smith guidance. *See* Combined code on corporate governance
Smithsonian agreement, 23
Société Générale, 286–290, 297
Society for establishing useful manufacturers, 248
SOP. *See* Standard operating procedures
SOX, 25, 28, 31, 33–34, 251, 257–258, 265, 276–277. *See also* SOX 404
  section 404 (*see* SOX 404)
SOX 404, 25–26, 28–29, 31, 33–34, 41, 276. *See also* SOX
Spain, 24
Standard operating procedures, 51, 68
State, 35–36
  and local government, 262, 266
  governments, 247
  governors, 55
  laws, 246
  tax, 9
Statement of financial accounting standards number 5. *See* SFAS 5
Strategic approach, 33, 228–229, 231
Stora, 246–247
Supply chain:
  operations reference model, 63, 93, 100, 116, 132, 202, 218 (*see also* SCOR)
  planning, 94–96, 98
  process, 116–119
Supply Chain Council, 63, 93, 132–133, 202
Sweden, 24, 246
Switzerland, 24, 173
SUM. *See* Society for establishing useful manufacturers
System failure. *See* Failure

Taxonomy, 121–124, 126, 159–160. *See also* MIT process handbook
Taylor, Fredrick Winslow, 55–58, 71
Technology, 19–20, 59–62, 107, 165, 265, 295
  existing, 51, 112, 152
  failure (*see* failure)
  information, 27, 60, 90, 134, 140, 174, 179, 202, 206, 294 (*see also* IT)
  inventory, 12, 293
  metrics, 140–141
  new, 112, 152
  organization (s), 219, 225–226, 232 (*see also* organization, IT)
  processing, 140

Technology (*continued*)
security, 22 (*see also* security)
solutions, 12, 175, 178, 183, 293
role of, 163, 169
tools, 194, 268
Telemanagement Forum, 63
TJ Maxx, 130
TJX, 130–131, 144
Tone from the top, 42, 81–86, 129, 134, 160, 278, 280, 282. *See also* Risk objectives
Total quality control. *See* TQC
Total quality management. *See* TQM
TQC, 53, 58, 70
TQM, 53, 58–60, 70, 294
Training, 20, 24, 51, 107, 142, 200, 227, 230–231, 243, 279–280
Treadway Commission, 23, 34, 47, 134, 144. *See also* COSO
Treadway, James, 23
Treasury, Department of, 278, 284
Turnbull guidance. *See* Combined code on corporate governance
Turnbull, Nigel, 257
Tyco, 25
Tylenol (incident/scare), 84, 100, 223

UCTE, 173, 196
UK (U.K.), 186, 246. *See also* United Kingdom
department of trade and industry, 58
Unencrypted, 37
Unexpected risk
Unfortunate events
Union for the co-ordination of transmission of electricity. *See* UCTE
United Kingdom, 24, 247–257, 260. *See also* UK
United States, 24, 31, 33, 35–36, 58, 105, 130, 142, 146, 171–172, 198–199, 220, 222, 246, 247, 249, 257–258, 260, 276, 279, 286. *See also* U.S.
Universal business standards, 215
Universal process classification scheme, 61
U.S.
armed forces, 227
companies/corporations, 25, 29, 33, 35, 45, 59, 82, 147, 198, 246–247, 260
Congress, 105, 199, 248, 251
department of health and human services (*see* health and human services)
department of labor (*see* labor)
Federal Reserve (*see* Federal Reserve)
food and drug administration (*see* FDA)
government accountability office (*see* GAO)
governance, 261
government, 147, 171, 221, 240, 249, 278
history, 17, 19, 249, 276
laws, 246
regulations, 24, 27, 250
regulatory agencies, 279
securities and exchange commission (*see* SEC)
standards, 199, 200

Validation, 42, 145, 163
Vendor, 10, 26, 36, 93, 107, 193–194, 200, 225. *See also* Outsource
Verifiable, 140
Verification, 40, 145–146, 163, 253
Verify (ing), 67, 145–146, 200, 211
Vigilance, 129, 163, 171, 236

Watkins, Sherron, 252
Websphere business modeler, 66
Whistleblower, 252–253, 270
blow the whistle, 32
WorldCom, 25, 249–252, 255–256, 260–262, 270, 277, 296
Wriston, Walter, 275
Wrong-side surgery, 220–223