A
Action tracking reporting, 230–233
Audit, 57

B
Bank of International
Settlements (BIS), 15–16
Basel Accords, 2–3, 5, 9, 15–28
Basel I, 17–18
Basel II, 2–3, 5, 9, 18–23,
93–102, 111–112, 189,
193, 211, 213, 215
business line categories, 111
European adoption of, 21
Pillar 1, 18–20
Pillar 2, 9, 21
Pillar 3, 21
risk event categories, 93
U.S. adoption of, 21–23
Basel Committee on Banking
Supervision, 42–45,
58, 73
Business continuity planning
(BCP), 54–55
Business continuity metrics, 151

C
Capital modeling, 189–217
advanced measurement
approach, 199–211
hybrid approach, 211
loss distribution approach
(LDA), 203–209
scenario analysis approach,
209–211
basic indicator approach
(BIA), 191–193
disclosure, 213–215
future of capital requirements,
215–216
insurance, 211–213
operational risk capital,
189–190
standardized approach,
193–199
alternative, 197–198
future of, 198–199
Chief administrative officer
(CAO), 49–50
Chief compliance officer, 50–51
Chief financial officer (CFO),
49–50
Chief operating officer (COO),
49–50
Chief risk officer (CRO), 46–49
Citi, 3
Client metrics, 151
Coe, Lord Sebastian, 5, 8
Compliance metrics, 148–149
Credit Suisse annual report
(2011), 213–214
Culture and awareness, 63–75
marketing and communication, 64–65
planning, 66–71
major deliverables checklist, 67–71
sample project milestones, 72
success of framework, 63
training, 65–66
“use test,” 71–74

D
Deliverables, checklist, 67–71
Deutsche Bank annual report (2011), 214
Dodd-Frank Act, 26–28

E
Enterprise risk management (ERM) wheel, 11
Exception monitoring, 143
External loss data, 121–140
challenges of, 134–139
Société Générale and the external event that shook the operational risk world, 135–139
comparisons between subscription and consortium databases, 129–134
frequency of losses by risk category, 131–132
number of events by business line, 134
size of losses by business line, 132–133
size of losses by risk category, 129–131
external operational risk event data, 121–122
external loss event data, sources of, 122–129
consortium data, 126–129
subscription databases, 123–126

F
Financial statement metrics, 152–153
Fraud risk management, 285

G
Governance, risk, and compliance (GRC), 270–278
assessment convergence, 271–275
converged data, 274
taxonomies, 274–275
tools, 275
convergence of metrics, 275–278
Group of Twenty (G20), 23

H
Hurricane Sandy, 256

I
Information security, 55
Internal loss data, 89–119
data collection, 114–116
operational risk event data, 89
internal operational risk events, 90–92
information collected in loss data program, 92
reasons for collecting data, 90–91
who should collect data, 91–92
minimum loss data standards, 102–114
action items, 113–114
amount, 103
boundary events identified, 113
business line, criteria for allocation to, 112
central function, criteria for allocation to, 112–113
comprehensive, 102
date, 108–110
description and causes, 110–112
impacted departments, 113
nonfinancial impacts, 114
threshold, 102–103
risk event categories, 93–102
Business Disruption and System Failures, 99–100
Clients, Products, and Business Practices, 97–98
Damage to Physical Assets, 98–99
Employment Practices and Workplace Safety, 96–97
Execution, Delivery, and Process Management, 100
External Fraud, 95–96
Internal Fraud, 94–95
using, 100–102

International Convergence of Capital Measurement and Capital Standards, a Revised Framework, 18

J
JPMorgan Chase, 3, 102, 114–115, 161–162
“whale” case study, 291–296

K
Kerviel, Jerome, 135–137
Key risk indicators (KRIs), 37–38, 141–154, 228–229
challenges, 147
exception monitoring, 143
key control indicators (KCIs), 143
key performance indicators (KPIs), 143
lagging indicators, 144
leading indicators, 144
metric examples, 147–153
business continuity, 151
client, 151
compliance, 148–149
financial statement, 152–153
people, 147–148
technology and infrastructure, 149–150
trade execution and process management, 152
reporting, 228–229
selecting, 145
standards, 146–147
thresholds, 146
Knight Capital technology glitch, 296–297, 313
L
Lagging indicators, 144
Leading indicators, 144
Legal risk management, 283
LIBOR scandal, 257–260
London Olympics (2012) case study, 4–8
Loss data collection, 36
Loss data standards, minimum, 102–114
action items, 113–114
amount, 103–108
accounting adjustments or timing events, 107
gains, near-misses, and opportunity costs, 106–107
indirect costs, 105–106
recoveries, 108
boundary events identified, 113
business line, criteria for allocation to, 112
central function, criteria for allocation to, 112–113
comprehensive, 102
date, 108–110
challenge for legal events, 108–110
description and causes, 110–112
impacted departments, 113
nonfinancial impacts, 114
threshold, 102–103

Measurement and modeling, 38
Metric examples, 147–153
business continuity, 151
client, 151
compliance, 148–149
financial statement, 152–153
people, 147–148
technology and infrastructure, 149–150
trade execution and process management, 152
Monte Carlo Simulation, 207–208

N
New business/product approval, 56
New-product appeal, 281–282

O
Operational risk capital, 189–190
reporting, 229–230
and convergence, 269–280
converged or GRC reporting, 278–280
governance, risk, and compliance (GRC), 270–278
operational risk as catalyst, 269–270
coordinators, 52–54
definition and drivers of, 1–14
2012 London Olympics case study, 4–8
definition, 1–4
drivers, 12–14

M
Marketing and communication, 64–65
Markets in Financial Instruments Directive (MiFID), 12
Index

management and measurement, 8–12
framework, 33–40
culture and awareness, 35
governance, 34–35
key risk indicators, 37–38
loss data collection, 36
measurement and modeling, 38
overview of, 33
policies and procedures, 35
reporting, 38
risk appetite, 39
risk and control self-assessment, 37
scenario analysis, 37
governance, 41–62
first line of defense, 44
risk committees, 59–61
role of, 41–44
second line of defense, 45–56
third line of defense, 57–58
reputational risk and, 255–268
definition of, 255–256
impact, 256–260
management framework, 262–266
regulatory oversight of, 261–262
“Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches” (2011), 58, 73
Operational Riskdata eXchange Association (ORX), 110–111

P
Pandemic planning, 287–288
People metrics, 147–148
Planning, 66–67
Policies and procedures, 77–88
best practices, 80
operational risk policy, 80–86
role of, 77–79
documentation hierarchy, 79
sample standards, procedures, and guidelines, 86–88
extract from loss data procedures document, 87
extract from loss data standards document, 86–87
linkage between documents, 87–88
Policy office, 56
“Principles for Enhancing Corporate Governance” (2010), 42–43, 47

R
Regulatory push, 15–31
Basel Accords, 15–23
European adoption of Basel II, 21
rules of, 17–21
U.S. adoption of Basel II, 21–23
financial crisis, impact of, 23–28
Basel III, promise of, 23
European response to, 24
U.S. response to, 24–28
future, 28
Regulatory risk management, 284
Related risk management
activities, best practices in, 281–290
fraud risk management, 285
legal risk management, 283
new-product appeal, 281–282
pandemic planning, 287–288
people risk management, 284–285
regulatory risk management, 284
strategic risk, 288–289
supplier and third-party risk, 282
technology risk management, 285–286
weather risk, 288

Reporting, 38, 219–235
action tracking, 230–233
capital, 229–230
consolidated view, 233, 234
dashboards, 233
key risk indicator (KRI), 228–229
loss data, 221–228
external, 227–228
impact of gains on, 221–223
internal losses by risk category, 225, 226
timeliness, 225, 227
trends in internal losses, 223–225
risk and control self-assessment, 228
role of, 219–221
scenario analysis, 229

Risk categories, 5–6
Risk appetite, 39, 237–253
current, 251
framework, implementing, 243–247
firmwide, promoting, 246
governance, 245–246
monitoring, 246–247
as strategic decision-making tool, 244–245
monitoring, 247–251
appetite, 248
capacity, 248
limits/indicators, 249–251
tolerance, 248–249
range of practice in, and tolerance methods, 242–243
regulatory expectations, 239–241
role of, 237–239

Risk and control self-assessment (RCSA), 37, 155–171, 228
best practices, 166–170
appropriate technology, implementing, 168
backtesting or validating results, 170
document results, 167
existing assessments, leveraging, 169–170
interviewing participants beforehand, 166
mitigating actions, identifying, 168
reporting, 228
review of available background data from other functions, 166
review of external events, 167
review of internal loss data, 166
review of past RCSAs and related RCSAs, 166
scheduling appropriately, 170
scoring methodology, 167
selecting and training participants, 167
taxonomies, ensuring completeness using, 168–169
themes identified, 169
methods, 158–162
hybrid, 161–162
questionnaire approach, 158–160
workshop approach, 160–161
role of assessments, 155–158
control assessments, 157
RCSAs, 158
risk and control assessments, 157
scoring methods, 162–166
control effectiveness, 162–163
probability or frequency, 165
risk impact, 163–165
risk severity, 165–166
Risk event categories, 93–102
Business Disruption and System Failures, 99–100
Clients, Products, and Business Practices, 97–98
Damage to Physical Assets, 98–99
Employment Practices and Workplace Safety, 96–97
Execution, Delivery, and Process Management, 100
External Fraud, 95–96
Internal Fraud, 94–95
using, 100–102
S
Sarbanes-Oxley Act (SOX), 12, 55–56
Scenario analysis, 37, 173–187, 229
approaches, 175–183, 209–211
appropriate representatives, 179
background preparation, 176–178
changes, process responsive to, 181–182
clearly defined and repeatable process, 176
documentation, 180–181
independent challenge and oversight, 181
mitigating biases, mechanisms for, 182–183
modeling operational risk capital, 209–211
qualified and experienced facilitators, 178–179
structured process for selection of data, 179–180
output, 183–186
reporting, 229
role of, 173–174
Securities and Exchange Commission (SEC), amendments to net capital rule, 21–22
Senior Supervisors Group (SSG), 242–243
Société Générale, 134, 135–139
Solvency II, 12
Standard Chartered anti–money laundering scandal, 297–300, 314
Strategic risk, 288–289
Supplier and third-party risk, 282

T
Technology and infrastructure metrics, 149–150
Trade execution and process management metrics, 152
Training, 65–66

U
UBS unauthorized trading scandal, 300–307
“Use test,” 71–74

V
Validation and verification, 58–59

W
Weather risk, 288