

- action plans 115–116, 118, 158, 164–165
- active errors 111–112
- advanced measurement approaches (AMA) 3–4, 13–18, 81–85
- aggregating risk data 160–163, 190
- anonymity 217–218
- approvals, project risk management 182–183
- assets
  - culture/behavior aspects 121–122
  - damage risk 21
  - inventories 197–199
  - project risk management 187
- asymmetry, loss data 166–169, 176–178
- attack risks 213, 215
- audits 10, 24, 98–101, 107–108, 135–137, 163–165
- availability aspects 66–67, 203
- averages, risk reporting 167–169
- banking/banks
  - cryptocurrency risk 207–219
  - culture/behavior aspects 121–122, 125–126
  - regulatory capital 77–92
  - risk appetite/tolerance 43
  - risk identification 31–32
- Basel categories 20–23, 25–27, 211–212, 214
- Basel Committee 77–82, 87, 115, 129–130, 161
- Basel II–III 77–92
- baselining operational risk 176–178
- basic indicator approach (BIA) 80
- Bayesian models 72–74
- behavior aspects 119–126, 164–165, 203–205
- BEICF *see* business environment and internal control factors
- benchmarking 169
- BIA *see* basic indicator approach
- biases 13–15, 65–67, 108–109
- Bitcoins 207–209, 213–219
- blockchains 207, 209–210, 212, 215–219
- board responsibilities 37–41, 44–47, 95, 101–102, 142–143
- bottom-up risk analysis 3–5, 9–10, 44–45
- boundary event reporting 136–137
- bow tie tool 116–118
- brainstorming 14–15
- breaches 41–48, 162–163, 193–196
- British road signs 146
- budgets 53–54, 181–187, 191–192
- building good reputations 222–223
- business continuity 203
- business disruption risk 22
- business environment and internal control factors (BEICF) 84, 143–144
- business ownership 95–97, 99–101
- business practice risk 21
- business values 175–178
- Cambridge Analytica 194–195
- capital
  - modeling/risk assessments 77–92
  - risk appetite 47–49
  - risk monitoring 129–132, 136, 143–144, 175
  - scenario analysis 63–65, 72–73, 84–92
- cascades 31–32
- categories
  - Basel risk levels 20–23, 25–27, 211–212, 214
  - cryptocurrency risk 210–212, 214
  - key risk indicators 146–149
  - risk reporting data aggregation 161
- cause analysis
  - causal indicators 148
  - risk identification 7–8, 14, 17, 19, 23–26, 29–33
  - risk management sequences xxii
  - risk management taxonomy 23–26

- cause analysis (*Continued*)
  - risk mitigation 115–118
  - scenario analysis 14, 17
- CCAR *see* comprehensive capital analysis and review
- Centre for Cyber Security 198–199
- change achievement, conduct/culture 122–126
- characteristics
  - key risk indicators 145–146
  - reputation risks 221–222
- circular presentation of risks *see* risk wheels
- clients' products & business practices 21
- climate change 29
- closure 184–185
- clusters 29–33
- colour-coded risk levels 46–47, 57–59
- competency 121–123, 226
- compliance risks 43, 157, 173–175
- comprehensive capital analysis and review (CCAR) 88–91
- comprehensive frameworks 41–42, 88–91
- conditional probability 72–74
- conduct
  - behavior aspects 119–126, 164–165
  - change achievement 122–126
  - definitions 119–120
  - risk appetite 43
  - risk mitigation 119–126
  - risk reporting 119, 124, 164–165
- confidential data 69–72
- confidentiality 203
- connectivity, risk identification 29–33
- consistency, conduct/culture 123–124
- consolidation, scenario analysis 75–76
- content aspects, risk reporting 157–158
- continuity testing 227
- controls
  - see also* risk and control self-assessments
  - information security risks 193–206
  - key risk indicators 144, 154–155
  - regulatory capital 84
  - risk appetite 41–45
  - risk management sequences xxiii
  - risk management taxonomy 24–27
  - risk mitigation 105–113, 115–118
  - testing 107–110
- conversion, data aggregation 160–163
- coordinated attack risks 213, 215
- core business processes 43
- corporate governance 37, 95, 99, 101–103
- corrective controls xxiii, 25, 106, 116–117
- COSO (Committee of Sponsoring Organizations) xx–xxi, 37, 42, 171
- credit risks 38–39, 151–152
- crime
  - confidential data 69–72
  - cryptocurrency risk 211, 214–219
  - cyber risks 193–198, 202, 211, 214–219
- crisis management 224–229
- cryptocurrency risk 207–219
  - anonymity 217–218
  - Basel categories 210–212, 214
  - Bitcoins 207–209, 213–219
  - blockchain 207, 209–210, 212, 215–219
  - crime 211, 214–219
  - double-spending risks 215–216
  - drivers 213–219
  - exposure 210, 213–219
  - irreversible transactions 216–217
  - losses/mistakes 216–217
  - mining strategies 209, 212, 215–216
  - risk identification 208–211, 214, 217–218
  - risk mitigation 210, 213–214
  - transaction verification 215–218
  - verification 215–218
  - virtual wallets 211–212, 215–217
  - vulnerabilities 210, 213–219
- “cube” framework xxi
- culture 119–126, 164–165
- currency risks 207–219
- cut-of mix, 83–84
- cyber risks
  - crime 193–198, 202, 211, 214–219
  - cryptocurrency 207–219
  - fraud 193–196, 211, 214–219
  - information security risks 193–206
  - risk identification 30, 33
  - theft 193, 197–198, 202, 211, 214
- cybersecurity *see* cyber risks
- damages 8, 21
- dashboards, risk reporting 164–165, 191

- data aggregation 160–163, 190
- databases 64–65, 129–132, 137–139
- data breaches 193–196
- data capture 150–155
- data collection 129–139
- data compromise 193
- data fields 132–134
- data losses 82–85, 166–169, 176–178
- data quality reviews 137
- data requirements, key risk indicators 150–151
- deadly sins 173–174
- debriefing 184–185
- debts 77
- decentralized governance 213, 215
- decision-making 98–101, 125–126, 157–158, 174–175, 181–182
- delivery and process management 22
- Delphi method 67–68
- design
  - key risk indicators 150–155
  - risk mitigation controls 109–113
- detective controls 25, 105–106, 116–117
- diamonds 29
- digital signatures 208–209
- directive controls 25, 106
- documentation
  - operational risk governance 102–103
  - scenario analysis 14, 74–76
- double-spending risks 215–216
- drivers, cryptocurrency risk 213–219
- duplicative controls 109
  
- earnings before interest and tax (EBIT) 186–187
- EBA *see* European Banking Authority
- ED *see* external data
- electronic currency risks 207–219
- employee data leaks 195–196
- employee interviews 10
- employment practice risks 20
- encryption 208, 212, 218
- enterprise risk management (ERM) xxi, 171
- environment influences, conduct/culture 123–124
- Equifax 194–195, 225
- ERM *see* enterprise risk management
- errors
  - cryptocurrency risk 212–218
  - key risk indicators 151–152
  - risk assessments 39, 42–43, 60
  - risk identification 19–22
  - risk mitigation 110–113
  - risk monitoring 144–152, 162, 167–168
- estimation biases 66–67
- European Banking Authority (EBA) 82
- European banks 31–32, 166, 176–178
- events
  - cryptocurrency risk 210–212
  - event templates 115
  - risk assessments 40–47, 52–58, 63–66, 69–75, 82–90
  - risk identification 6–7, 13–14, 19–26
  - risk management sequences xxii–xxiii
  - risk mitigation 96–97, 105–106, 112–113, 115–123
  - risk monitoring 129–139, 174–177
  - risk reporting 163–169
- examination controls 107
- excess risk analysis 47–49
- execution/delivery 22
- expert judgment 65, 67–68
- exposure
  - cryptocurrency risk 210, 213–219
  - key risk indicators 147–149
  - risk appetite 45
  - risk identification tools 5–6
  - risk management sequences xxii
- external data (ED) 83–85
- external fraud 20
- external losses 10–11
  
- Facebook scandal 194–195
- factor models 86
- failures
  - key risk indicators 148
  - risk identification 22
  - systematic patterns 116–118
- fault tree analysis (FTA) 67–74
- feedback assessments 171
- filtering 83–84
- flash questionnaires 199–201
- follow-up aspects 96–97, 118, 158, 174
- framework alignment 46–49, 59–61

- fraud
  - confidential data selling 69–72
  - crisis management 226
  - cryptocurrency risk 211, 214–219
  - cyber risks 193–196, 211, 214–219
  - risk identification 20
- frequency assessments 64–65, 87
- frequency of testing 108–109
- frequent data losses 166–167
- front-line risk management 95–97
- FTA *see* fault tree analysis
- FTSE 100 insurance company 4, 16
- funnel structures 40–41
- future directions 232–233
  
- general ledgers 137–138
- generation phases, scenario analysis 15–18
- geopolitical risks 32–33
- Glass-Steagall Act in 1999 (repeal of) 78–79
- golden rules 157, 173–174
- good reputations 222–224
- governance
  - action plan design 118
  - cryptocurrency risk 213, 215
  - key risk indicators 153–154
  - operational risk 95–103
  - project risk management 181–182, 185, 192
  - risk mitigation 118
  - scenario analysis 13–14
- Great Depression 77
- gross income benchmarks 169
  
- hacking incidents 225
- heatmaps 46–47, 57–59
- history, regulatory capital 77–79
- human error 110–112, 116, 151–152
- hybrid models, regulatory capital 86
  
- ICAAP *see* Internal Capital Adequacy Assessment Process
- IFRS Standards 79
- ILD *see* internal loss data
- IMA *see* internal modeling approaches
- impacts
  - definitions 53–54
  - RCSA exercises 53–59
  - risk management sequences xxiii
  - risk management taxonomy 23–26
  - scenario analysis 63–65, 72–76
- incentives
  - conduct/culture 122
  - risk reporting 135–136
- incident data collection
  - data fields 132–134
  - losses 129–139
  - non-financial impact fallacy 130–132
  - processes 132–139
  - regulatory requirements 129–132, 136–137
  - reporting 129–139
  - resistance 134–136
  - reviews 137–139
  - risk monitoring/reporting 129–139
  - self-reporting incentives 135–136
  - validation 137–139
- incident management xxiii, 197
- influence aspects, conduct/culture 123–124
- information asset inventories 197–199
- information disclosures 78
- information security risks (ISR) 193–206
  - asset inventories 197–199
  - behavior aspects 203–205
  - breaches 193–196
  - controls 193–206
  - crisis management 225–226
  - cyber risks 193–206
  - key risk indicators 205–206
  - leaked data 193–196
  - media reports 193–196
  - questionnaires 199–201
  - RCSA 200, 202
  - reputation risks 193, 195, 197–198
  - risk assessments 199–203
  - risk identification 197–199
  - risk mitigation 199–201, 203–205
  - scenario analysis 200, 203
  - standards 196–197
  - surveys 199–203
  - taxonomy 197–199
  - technical measures 203–205
  - third party risks 193, 195, 197–198
- information technology (IT) 138, 193

- inquiry controls 107
- insurance, risk mitigation 100–101, 110, 112–113
- insurance companies
  - information security risks 195–196
  - risk appetite 46–47
  - scenario generation phase 16
  - sur-solvency 46–47
  - top-down risk identification 4
- integrity 203
- internal audits 98–99
- Internal Capital Adequacy Assessment Process (ICAAP) 5, 88–91
- internal controls 24, 84, 105–113
- internal databases 82–83
- internal fraud 20, 226
- internal loss data (ILD) 82–85
- internal losses 10–11, 82–85
- internal modeling approaches (IMA) 16, 81–85
- international asset management firms 121–122
- international banks 121–122
- international financial firms 43
- International Organization for Standardization (ISO)
  - ISO 31000 xx–xxi, 171
  - ISO/IEC 27001 196
  - risk mitigation 105
- interviews 4, 10
- inventories 197–199
- investment companies 72–74, 89–90
- involvement stages, project risk management 181–185
- irreversible transactions 216–217
- ISO *see* International Organization for Standardization
- ISR *see* information security risks
- IT *see* information technology
- key control indicators (KCI) 144
- key performance indicators (KPI) 47, 144
- key risk indicators (KRI)
  - BEICF requirements 143–144
  - board responsibilities 142–143
  - categories 146–149
  - characteristics 145–146
  - controls 144, 154–155
  - data capture 150–155
  - design 150–155
  - errors 151–152
  - exposure 147–149
  - failure indicators 148
  - features of 145–146
  - governance 153–154
  - information security risks 205–206
  - number requirements 150–151
  - performance 144
  - preventive controls 154–155
  - project risk management 192
  - risk appetite 46–47, 141–145
  - risk monitoring 129–130, 139, 141–155
  - risk reporting 158, 160–163
  - roles 141–144
  - selection phases 150–151
  - stress/stretch 148
  - thresholds 145–146, 151–154
  - validation 146, 154–155
- knowledge-based errors 111
- KPI *see* key performance indicators
- KRI *see* key risk indicators
- lagging indicators 10–11, 145–146, 149
- large data losses 166–167
- latent errors 111–112
- LDA *see* loss distribution approaches
- leaked data 193–196
- leasing companies 8
- legal & compliance risks 43
- level 1 risk categories 20–23, 25–27, 211–212
- level 2 risk categories 20–23, 25–27, 211–212, 214
- level 3 risk categories 20–23, 214
- life cycles, project risk management 182
- likelihood ratings 53–59
- loss data 82–85, 166–169, 176–178
- loss distribution approaches (LDA) 85–88
- losses
  - cryptocurrency risk 216–217
  - incident data collection 129–139
  - regulatory capital 77–92
  - risk appetite 46–47
  - risk identification 10–11
  - risk management taxonomy 23–24
  - risk reporting 129–130, 166–169

- macroeconomic stress testing 91
- maintaining good reputations 223–224
- management
  - reputation risks 221–229
  - risk identification xxiv, 3–11
  - scenario analysis 63–64, 73, 75–76
- market infrastructure companies 27, 43
- market risks 38–39
- maturity assessments 171–178
- MECE *see* Mutually Exclusive and Collectively Exhaustive
- median 168
- media reports 193–196
- mentors 123
- metrics, risk reporting 164–165
- mining companies 29–31
- mining strategies 209, 212, 215–216
- mis-selling risks 43
- mistakes/errors
  - cryptocurrency risk 216–217
  - risk mitigation 111
- modeling regulatory capital risks 77–92
- modern representations, RCSA 58–59
- Monte Carlo simulations 73–74, 87
- Mutually Exclusive and Collectively Exhaustive (MECE) 23, 25–26
  
- natural disasters 225
- near misses 10–11, 115–116, 118
- networks, risk identification 25–33
- no average in risk 167–169
- non-financial impact fallacy 130–132
- Nordic bank 135
- number requirements, key risk indicators 150–151
  
- objectives, RCSA exercises 51–53
- observation controls 107
- occurrence impacts/probability 51, 53–60, 64–65, 72–74
- operational risk capital modeling 77–92
- Operational Risk Consortium (ORIC) 17–18, 83, 166
- Operational Riskdata eXchange Association (ORX) 17–18, 83, 166
  
- operational risk governance
  - audits 98–99
  - board responsibilities 95, 101–102
  - committees 101–103
  - documentation 102–103
  - internal audits 98–99
  - organization aspects 101–103
  - ownership 95–97, 99–101
  - partnership models 100–101
  - policies 102–103
  - procedures 102–103
  - risk committees 101–103
  - risk functions 97–101
  - risk mitigation 95–103
  - three lines of defense model 95–102
- operational risks
  - future directions 232–233
  - Pillar 1 78–88
  - RCSA exercises 51–57, 182, 187, 190–191, 199–203
  - regulatory capital 78–88
  - risk appetite 38–42, 45–46, 49
  - risk connectivity 29, 32–33
  - risk definition and taxonomy 19, 22–26
  - risk identification 5, 8, 10–11, 29, 32–33
  - risk monitoring 171–178
  - risk networks 29, 32–33
  - scenario analysis 13–18
- optimistic controls 109
- organization aspects 101–103
- ORIC *see* Operational Risk Consortium
- ORX *see* Operational Riskdata eXchange Association
- outages 73–74, 226
- ownership of risks 95–97, 99–101
- own funds 77
  
- Paradise Papers 194
- partnership models 100–101
- peer-to-peer systems 207–219
- people environment influences 123
- performance, key risk indicators 144
- performance controls 108, 144
- personal values 122
- physical asset damage 21
- physical environment influences 123–124

- platform outages 73–74
- policies
  - project risk management 184–185
  - risk governance 102–103
- pooling expert judgment 67–68
- portfolios 183–184
- preparation phases, scenario analysis 13–14
- preventive controls
  - key risk indicators 154–155
  - risk management sequences xxiii
  - risk management taxonomy 24
  - risk mitigation 24, 105–106, 110–113, 116–117
- primary controls 106
- PRINCE 2 181–182
- probability of occurrence 51, 53–60, 64–65, 72–74
- procedures, operational risk governance 102–103
- processes, incident data collection 132–139
- process mapping 4, 9
- progress assessments 124–125
- project risk management 181–192
  - approvals 182–183
  - closure 184–185
  - data aggregation 190
  - debriefing 184–185
  - decision-making 181–182
  - governance 181–182, 185, 192
  - key risk indicators 192
  - life cycles 182
  - policy 184–185
  - portfolios 183–184
  - ratings 186–189
  - RCSA 182, 187, 190–191
  - risk assessments 181–182, 187–190
  - risk function 181–187
  - risk identification 181–182, 187–190
  - risk mitigation 182
  - risk monitoring 182, 191–192
  - risk ratings 186–189
  - risk reporting 191–192
  - risk update 182
  - stage-gate processes 181–182
- propinquity 123–124
- pyramid structures 46–47
- QIS *see* quantitative impact studies
- quality assessments 172
- quality reviews 137
- quantification details 73–74
- quantitative impact studies (QIS) 80
- quartiles 168
- questionnaires 199–201
- rare data losses 166–167
- RCSA *see* risk and control self-assessments
- reconciling, risk identification tools 5
- regulations, incident data collection 129–132, 136–137
- regulatory capital
  - advanced measurements 81–85
  - banks 77–92
  - Basel II 77–92
  - BEICF 84
  - calculation datasets 82–83
  - CCAR process 88–91
  - control factors 84
  - external data 83–85
  - frequency assessments 87
  - history 77–79
  - ICAAP 88–91
  - internal databases 82–83
  - losses 77–92
  - modeling 77–92
  - Monte Carlo simulations 87
  - operational risks 78–88
  - Pillar 1 78–88
  - Pillar 2 78, 88–92
  - rationale 77–79
  - risk assessments 77–92
  - scenario analysis 63–65, 72–73, 84–86, 89–92
  - severity assessments 87
  - standardized measurement 79–81
  - stochastic models 85
  - stress testing 90–92
  - supervisory reviews 78, 88–92
  - units of measure 88
  - wind-down planning 92
- regulatory compliance 157, 173–174
- reperformance controls 108
- repetitive controls 109–110
- reputation 221–229
  - benefits 224

reputation (*Continued*)

- characteristics 221–222
- creating 222–223
- crisis management 224–229
- definition 221
- good reputations 222–224
- information security risks 193, 195, 197–198
- maintenance 223–224
- management 221–229
- risk appetite 44

residual risk self-assessment (RSA) 51

resignations 149

resilience 221–229

- crisis management 224–229
- definitions 224

resistance, risk reporting 134–136

retail banks 43

revenue impacts 8

reverse stress testing 92

reviews, incident data collection 137–139

rewards, risk appetite 38–39

risk, definitions xix–xx, 19–27

risk appetite

- board responsibilities 37, 39–41, 44–47
  - bottom-up risk analysis 44–45
  - comprehensive frameworks 41–42
  - controls 41–45
  - definitions 37–40
  - excess risk analysis 47–49
  - framework alignment 46–49
  - key risk indicators 46–47, 141–145
  - operational risk governance 98
  - rewards 38–39
  - risk assessments 37–49, 98
  - risk limits 41–44
  - risk management frameworks 46–49
  - risk management tools 42, 46
  - risk reporting 158, 160–162
  - risk tolerance 41–47
  - structures 39–49
  - top-down risk analysis 44–45
- risk assessments xxi, xxiii–xxiv, 35–92
- capital 77–92
  - cryptocurrency risks 208
  - heatmaps 46–47, 57–59
  - information security risks 199–203

modeling 77–92

- operational risk capital modeling 77–92
- project risk management 181–182, 187–190
- RCSA exercises 46–47, 51–61, 65, 84–85
- regulatory capital 77–92
- risk appetite 37–49, 98
- risk management frameworks xxi, 46–49, 59–61
- scenario analysis 63–76

risk-based control testing 108–109

risk champions 97

risk clusters 29–33

risk committees 101–103

risk connectivity 29–33

risk and control assessment (RCA) 51, 159

risk and control self-assessments (RCSA)

- framework alignment 59–61
- heatmaps 46–47, 57–59
- impact ratings 53–59
- incident data collection 129–130
- information security risks 200, 202
- likelihood ratings 53–59
- matrix 46–47, 57–59
- modern representations 58–59
- objectives 51–53
- occurrence impacts/probability 51, 53–60
- operational risks 182, 187, 190–191, 199–203
- probability of occurrence 51, 53–60
- project risk management 182, 187, 190–191
- risk appetite 46–47
- risk assessments 46–47, 51–61, 65, 84–85
- risk identification tools 3–4
- risk management frameworks 59–61
- risk mitigation 100, 108, 116
- risk monitoring 129–130, 153, 160, 173
- structures 51–53

risk functions 97–101, 181–187

risk governance 95–103, 153–154

risk identification xxi, xxiii–xxiv, 1–33

- bottom-up risk analysis 3–5, 9–10
- cause analysis 7–8, 14, 17, 19, 23–26, 29–33
- clusters 29–33
- connectivity 29–33
- cryptocurrency risk 208–211, 214, 217–218
- exposure 5–6
- information security risks 197–199



- interviews 4, 10
- lagging indicators 10–11
- losses 10–11
- management tools xxiv, 3–11
- near misses 10–11
- networks 25–33
- process mapping 4, 9
- project risk management 181–182, 187–190
- risk appetite 49
- risk clusters 29–33
- risk connectivity 29–33
- risk lists 8, 25–27, 29–31
- risk networks 25–33
- risk registers 27, 29–30, 33
- risk wheels 6–8
- root causes 8
- scenario analysis 3–4, 13–18
- taxonomy 23–27
- tools xxiv, 3–11
- top-down risk analysis 3–5
- vulnerabilities 5–6
- risk limits 41–44
- risk lists 8, 25–27, 29–31
- risk management
  - actions xxiii–xxiv
  - frameworks xx–xxi, 46–49, 59–61, 171–178
  - scenario analysis 63–64, 73, 75–76
  - sequences xxi–xxiii
  - taxonomy 23–27
  - tools xxiv, 3–11, 42, 46
- risk mitigation 93–126
  - action plans 115–116, 118
  - bow tie tool 116–118
  - cause analysis 115–118
  - conduct 119–126
  - controls 105–113, 115–118
  - corrective controls 25, 106, 116–117
  - cryptocurrency risk 210, 213–214
  - culture 119–126
  - definitions 105
  - design of controls 109–113
  - detective controls 25, 105–106, 116–117
  - events 115–118
  - failure systematic patterns 116–118
  - follow-up 96–97, 118
  - good practice 115–116
  - governance 118
  - human error 110–112, 116
  - information security risks 199–201, 203–205
  - insurance 100–101, 110, 112–113
  - internal controls 105–113
  - near misses 115–116, 118
  - operational risk governance 95–103
  - preventive controls 24, 105–106, 110–113, 116–117
  - project risk management 182
  - RCSA exercises 100, 108, 116
  - risk management actions xxiii–xxiv
  - risk management frameworks xxi
  - risk management tools xxiv
  - risk transfers 105, 112–113
  - root cause analysis 115–118
  - systematic patterns of failure 116–118
  - target culture 120–126
  - testing controls 107–110
  - transfers 105, 112–113
  - types of controls 105–113
- risk monitoring 127–178
  - baselining operational risk 176–178
  - business values 175–178
  - capital 129–132, 136, 143–144, 175
  - compliance 157, 173–175
  - data collection 129–139
  - deadly sins 173–174
  - errors 144–152, 162, 167–168
  - follow-up 158, 174
  - golden rules 157, 173–174
  - incident data collection 129–139
  - key risk indicators 129–130, 139, 141–155
  - maturity assessments 171–178
  - ORM maturity 171–178
  - project risk management 182, 191–192
  - quality assessments 172
  - RCSA exercises 129–130, 153, 160, 173
  - reporting separation 159–160
  - risk management actions xxiii–xxiv
  - risk management frameworks xxi, 171–178
  - risk management tools xxiv
  - risk reporting 129–139, 157–169
- risk networks 25–33
- risk ownership 95–97, 99–101

- risk ratings 186–189
- risk registers 27, 29–30, 33
- risk reporting
  - action plans 158, 164–165
  - aggregating risk data 160–163
  - averages 167–169
  - behavior aspects 119, 124, 164–165
  - benchmarking 169
  - boundary events 136–137
  - challenges 158–164
  - conduct 119, 124, 164–165
  - content aspects 157–158
  - dashboards 164–165
  - data aggregation 160–163
  - data losses 166–169
  - golden rules 157
  - gross income benchmarks 169
  - incentives 135–136
  - incident data collection 129–139
  - key risk indicators 158, 160–163
  - losses 129–130, 166–169
  - monitoring separation 159–160
  - no average in risk 167–169
  - project risk management 191–192
  - risk appetite 158, 160–162
  - risk monitoring 129–139, 157–169
  - rules 157
  - story creation 169
- risk tolerance 41–47
- risk transfers 105, 112–113
- risk update 182
- risk wheels 6–8
- rogue trading 226
- root cause analysis 8, 115–118
- RSA *see* residual risk self-assessment
- rules
  - conduct/culture 124
  - risk reporting 157
- safety, Basel categories 20
- sampling 109
- Sarbanes–Oxley (SOX) regulations 107
- scaling, loss data 83–84
- scenario analysis
  - advanced measurements 3–4, 13–18
  - anchoring 66
  - Bayesian models 72–74
  - biases 13–15, 65–67
  - capital 63–65, 72–73, 84–92
  - cause analysis 14, 17
  - conditional probability 72–74
  - consolidation 75–76
  - Delphi method 67–68
  - documentation 74–76
  - estimation biases 66–67
  - expert judgment 65, 67–68
  - fault tree analysis 67–74
  - frequency assessments 64–65
  - generation phases 15–18
  - governance phases 13–14
  - impact assessments 63–65, 72–76
  - information security risks 200, 203
  - investment companies 72–74
  - management 63–64, 73, 75–76
  - Monte Carlo simulations 73–74
  - occurrence probability 64–65, 72–74
  - outages 73–74
  - preparation phases 13–14
  - quantification detail 73–74
  - regulatory capital 63–65, 72–73, 84–86, 89–92
  - risk assessments 63–76
  - risk identification 3–4, 13–18
  - risk management 63–64, 73, 75–76
  - scenario data 84
  - scenario sheets 74–75
  - scenario stress testing 90–91
  - selection phases 15–18
  - severity assessments 63–64
  - systematic estimation 66–67
  - validation 63, 74–76
- scoring mechanisms 160–163
- secondary controls 106
- security risks 193–206
- selection phases
  - key risk indicators 150–151
  - scenario analysis 15–18
- self-assessments *see* risk and control
- self-assessments
  - self-assessments
- self-certification controls 107
- self-reporting incentives 135–136

- sensitive information 218
- sensitivity stress testing 90
- sequences of risk management xxi–xxiii
- service level agreements (SLA) 144
- severity assessments 63–64, 87
- SIFI *see* systemically important financial institutions
- SLA *see* service level agreements
- slips/errors 111
- SMA *see* standardized measurement approach
- Sound Management of Operational Risk 78, 80–81, 115, 161
- SOX *see* Sarbanes–Oxley regulations
- staff interviews tools 10
- staff turnover 149
- stage-gate processes 181–182
- standalone databases 137–139
- standardized measurement approach (SMA) 79–81, 130, 136
- standards
  - information security risks 196–197
  - ISO standards xx–xxi, 105, 171, 196
- stochastic models 85
- story creation, risk reporting 169
- strategic objectives 37–49
- stress, key risk indicators 148
- stress testing 90–92
- stretch, key risk indicators 148
- structures
  - RCSA exercises 51–53
  - risk appetite 39–49
- supervisory review processes 78, 88–92
- sur-solvency 46–47
- surveys 32–33, 199–203
- systematic estimation 66–67
- systematic patterns of failure 116–118
- system failures 22
- systemically important financial institutions (SIFI) 78
- system outages 226
- systems uptime 203
- target culture 120–126
- taxonomy
  - definitions 23–27
  - information security risks 197–199
  - risk definitions 23–27
  - risk identification 23–27
- TDRA *see* top-down risk analysis
- technical measures, information security risks 203–205
- theft, cyber risks 193, 197–198, 202, 211, 214
- third party risks
  - information security risks 193, 195, 197–198
  - reputation 44, 193, 195, 197–198, 225
- three lines of defense model (3 LoD) 95–102
- three-pillars approach 77–78
- thresholds, key risk indicators 145–146, 151–154
- top-down risk analysis (TDRA) 3–5, 44–45
- transaction verification 215–218
- transfers, risk mitigation 105, 112–113
- transparency 226
- uncoverable losses/mistakes 216–217
- units of measure (UoM) 88
- validation
  - incident data collection 137–139
  - key risk indicators 146, 154–155
  - scenario analysis 63, 74–76
- value, risk management frameworks 175–178
- velocity, RCSA exercises 51
- verification, cryptocurrency risk 215–218
- violations 111
- virtual currency risks 207–219
- virtual wallets 211–212, 215–217
- vulnerabilities
  - cryptocurrency risk 210, 213–219
  - risk identification tools 5–6
- WEF *see* World Economic Forum
- willingness, conduct/culture 122
- wind-down planning 92
- workplace safety 20
- workshops 14, 51
- World Bank war room training sessions 227–228
- World Economic Forum (WEF) risk network 29





