

Index

- Accounting, 135, 145
- Accounts receivable, 102, 120, 150, 190, 214, 215, 225, 226
- Administration
 - key outcomes, 134–139
 - KRIs, 145–149
 - physical mapping, 123–125
- Analytics, 30, 209. *See also* Business risk analysis techniques (BRATs)
- Audits, 204, 213, 214, 226, 227, 229, 230, 239, 264
- Automation
 - ERM environment, 14, 29, 31, 211, 220–222
 - of KRIs, 153–168
 - outsourcing oversight, 243, 246
 - physical mapping, 43
 - profiling, 192
 - risk assessment tools, 209, 211, 212
 - and risk indicators, 117, 120, 121, 134, 153
 - risk management, 95, 112, 192
 - SOX compliance, 265, 266
- BADMAN (bad manager) profile, 90, 95
- BADSYS (bad system) profile, 89, 95
- Banking industry
 - bank tellers, 260, 261
 - business risk, 35, 64, 65
 - cash deposits and money laundering, 193
 - corporate image risk, 68
 - defining the business, 35, 38, 39
 - key early warning indicators, 115. *See also* Key early warning indicators (KEWIs)
 - logical data pathways, use of, 200–202
 - OCC risk categories, 64
 - pivotal point of change analysis, 180
 - real-time profiling, 214, 217
 - and risk appetite, 28
 - and Sarbanes-Oxley, 15
 - trend analysis, 178, 179
 - universal risk indicators, 89
- Baseline for risk categories, 64–74
- Baseline metrics for outsourcing, 241
- Baseline risk register, 169, 170
- Benchmarking, 25, 26, 33, 81
- BRAIN (Business Risk Assessment Information Network), 33–37, 202
- BRATS. *See* Business risk analysis techniques (BRATs)
- Budget process, 102–104
- Business
 - core business processes, 40–52
 - defining, need for, 38–40
 - physical mapping, 42–52. *See also* Physical mapping
 - structure, 41, 42, 46, 48–52, 76, 77, 79, 81
 - understanding, need for in systems design, 206
- Business Planning, 138, 139, 147, 148
- Business processes
 - core processes, 40–52
 - outcomes, 59–62. *See also* Outcomes
 - outputs, 59–62, 98
- Business risk analysis techniques (BRATs), 119, 120, 178–200, 209
- Business Risk Assessment Information Network (BRAIN), 33–37, 202
- Business risk, defining, 59–77, 206, 207
- Business/organizational risk, 260, 261
- Call centers, 174–176, 240
- Change, 203
- Chief Executive Officer (CEO), 29, 92, 219, 224, 264
- Chief Information Officer (CIO), 7, 29, 204, 219
- Chief Risk Officer (CRO), 27, 29, 35, 204, 219, 260, 261
- Coderre, Dave, 224
- Committee of Sponsoring Organizations (COSO)
 - cubes, 16–22
 - ERM framework, 14–22, 88
 - framework for SOX compliance, 2, 3, 14–22

272 ■ Index

- Comparative analysis, 183–200, 209
- Confidentiality risk, 65, 69–71, 129, 130
- Construction industry fraud, 195, 199, 200
- Continuous auditing, 224
- Continuous evaluation of risk, 11, 31, 52, 62, 81, 90, 219, 224. *See also* Dashboard indicators; Key Risk Indicators (KRIs)
- Control environment, 18, 19, 208
- Core business processes, 40–52
- Corporate culture, 28, 29
- Corporate image, 65, 67, 68
- Costs
 - audit fees, 226, 227
 - cost concentration, 100, 101
 - economies of scale and cost benefits, 221, 222, 226–228
 - outsourcing, savings from, 13, 14
- Courier services, 129, 130
- Credit cards, 217
- Credit memos, 120
- Credit risk, 35, 38, 39, 202
- Crisis management, 266
- Critical support units (CSUs), 41, 42, 104, 232, 236, 237
- Customer satisfaction, 39, 172–175, 240
- Dashboard indicators, 111–115
- Data
 - analysis, 10, 11, 76, 193, 195
 - and automation, 120, 121
 - and benchmarking, 81
 - confidentiality. *See* Confidentiality risk
 - data-centric ERM. *See* Data-centric ERM (DCERM)
 - integrity. *See* Data integrity and reliability
 - limitations on, 120, 121
 - logical data pathways. *See* Logical data pathway (LDP)
 - Outcome/Raw (O/R) data, 94–98, 177, 178, 207
 - patterns, 193, 195
 - raw versus blended data, 95–98
 - sources of, 99
 - and systems design, 207, 208
 - use of to define risk, 80–86
- Data integrity and reliability, 8, 10, 65, 69, 77, 99, 168, 202, 262
- Data-centric ERM (DCERM)
 - automation, 29
 - business value, 221–224
 - and COSO/ERM, 20, 88
 - and cost reductions, 226–228
 - data, amount of, 120, 121
 - DREAM (Data-Centric Risk Evaluation Assessment and Management), 265–267
 - economies of scale and cost benefits, 221, 222, 226–228
 - importance of, 29, 30, 79, 92
 - overview, 87, 88
 - risk model, building. *See* Fluid/dynamic risk model
 - system-centric data-centric tools, 209, 212–219, 265
- Data-Centric Risk Evaluation Assessment and Management (DREAM), 265–267
- Disaster recovery/contingency planning risk, 65, 72, 73
- Distributed Risk Assessment and Management (DRAM), 77, 79
- DREAM HOME, 265–267
- Dynamically integrated risk evaluation (DIRE), 211–216, 265
- EARS (Embedded Audit and Risk System) Real Time Profiling, 214, 216–219
- Engineering, 108, 140, 141, 150
- Enron, 53, 66, 74
- ERM (enterprise risk management)
 - business value, 221, 222
 - and change, 203
 - corporate sponsorship, 27
 - COSO framework, 14–22, 88
 - data-centric. *See* Data-centric ERM (DCERM)
 - DREAM HOME, 265–267
 - fluid/dynamic risk model. *See* Fluid/dynamic risk model
 - focused outcome groups (FOGs), 173–175
 - future evolution of, 219, 220
 - and future prediction, 31, 32, 266, 267
 - governance, risk, and control (GRC), 14, 263, 264
 - Holistic Oversight Management Environment (HOME), 263–264
 - IT, alignment with, 31
 - modular approach, 172, 173
 - as organizational essential strategy (OES), 262, 263
 - ownership of risk management process, 260–262
 - qualities of effective ERM, 27–32
 - and risk models, 23–26
 - stakeholder involvement, 261, 262
 - and strategic initiatives, 263, 264
 - and systems design, 211, 219. *See also* Systems design
 - systems strategies, 204, 205
- Executive compensation, 195, 220
- Exxon Valdez*, 68
- Finance, 134, 145, 146, 153–155
- Financial risk, 35, 43, 65, 66, 154, 155, 249

- Fluid/dynamic risk model
 - dashboard indicators, 111–114
 - data used, 94–98
 - drivers for, 100–111
 - implementation of. *See* Implementation of fluid/dynamic risk model
 - key early warning indicators (KEWIs), 113, 115
 - and Key Risk Indicators. *See* Key Risk Indicators (KRIs)
 - need for, 92, 93
 - proactive versus reactive risk management, 93, 94
 - universal risk indicators, 117–120
- Focused outcome group (FOG), 173–175
- FORT (financial, operational, regulatory, and technological) KRIs, 112, 120, 121
- Fraud, 102, 193, 195–200, 217, 258, 259
- Global technology audit guide (GTAG), 224
- Governance, designing risk-centric systems for, 205–211
- GRC (governance, risk, and compliance), 14, 263, 264
- Health Insurance Portability and Accountability Act (HIPAA), 36, 70, 161, 164
- Healthcare industry
 - comparative analysis, use of, 184, 185
 - confidentiality risk, 36, 70, 71. *See also* Confidentiality risk
 - fraud, 195–199
 - HIPAA, 36, 70, 161, 164
 - physical mapping example, 43–52
- Human Resources (HR)
 - and business structure, 41, 125
 - key outcomes, 136–138
 - Key Risk Indicators (KRIs), 147
 - outsourcing, 244, 245
 - related risk example, 62, 63
 - risk, 136–138
- Impact analysis, 7, 8, 52–58, 82, 86, 88
- Implementation of fluid/dynamic risk model
 - baseline risk register, 169, 170
 - business risk analysis techniques (BRATs), 177–200
 - business risks, defining, 133–144
 - focused outcome group (FOG), 173–176
 - Key Risk Indicators (KRIs), 144–168
 - logical data pathways (LDPs), use of, 200–202
 - modular approach, 172, 173
 - net risk versus residual risk, 175, 177
 - overview, 122, 123
 - physical mapping, 123–133, 169–172
- Industry specific risk, 65, 68, 69
- Internal control, 2, 3, 14–23, 208, 224–226
- Inventory control (IC), 142, 151
- Inventory turnover, 106–111
- Investment management, 116, 117
- IT (Information Technology) department
 - alignment with ERM, 31
 - key outcomes, 138
 - KRIs, 147, 165–168
 - and outsourcing, 236, 237. *See also* Outsourcing
 - physical mapping of, 125–130
 - physical risks and metrics, 130
 - universal risk profiles, use of, 89
- Janitorial services, 126, 127
- Johns Manville Corp., 53
- Key early warning indicators (KEWIs), 113, 115
- Key Process Indicators (KPIs), 30, 59, 88, 98
- Key Risk Indicators (KRIs)
 - administration, 145–149
 - detailed inventories of for automated systems, 153–168
 - determining, 115–117
 - developing, 144–153
 - financial, operational, regulatory, and technological (FORT), 112, 120, 121
 - in fluid/dynamic risk model, 98–100
 - and key outcomes, 145
 - and net risk, 177
 - and operational outcomes, 84, 85
 - operations, 149–153, 156–161
 - as part of effective ERM, 29, 30
 - raw data versus blended data, 95–98
 - regulatory compliance, 161–165
 - risk registers. *See* Risk register
- Legal liability, 55, 65–67, 135, 136, 146
- Lehman Brothers, 53, 93
- Leonard Vona and Associates, 193, 194
- Logical data pathway (LDP), 42, 77, 78, 106, 123, 172, 200–202, 222
- Machinery maintenance, 54–58
- Maintenance and installation services, 127, 128
- Management, universal risk profile, 89, 90
- Manufacturing, 106–111, 143, 151, 152, 222, 223
- Mean dispersion analysis (MDA), 181, 182
- Mergers and acquisitions (M&As), 138, 139, 228–234
- Merrill Lynch, 93

274 ■ Index

- Metric Oversight Monitoring Systems (MOMS), 212–216, 265
- Microsoft, 67
- Microsoft Excel, 169
- Microsoft Visio, 170
- Modular approach, 172, 173
- MOMS (Metric Oversight Monitoring Systems), 212–216, 265
- Money laundering, 193
- Monitoring, 224–227, 240
- MORE (Multiplied Organizational Risk Effect), 53–58, 88
- Multi-Dimensional Risk Assessment, 88–91
- Multi-level Risk Ownership (MRO), 50–52
- Multiplied Organizational Risk Effect (MORE), 53–58, 88

- NASA, 69
- Net risk, 175, 177

- OCC (Office of the Comptroller of the Currency), risk categories, 64
- Offshoring. *See* Outsourcing; Ventoro Offshore 2005 Research Preliminary Findings and Conclusions
- On-site oversight (OSO), 243, 257
- Operations
 - key outcomes, 139–144
 - KRIs, 149–153, 156–161
 - physical mapping of, 131–133
 - risk, 65, 73, 74
- OR (Outcome/Raw) data, 94–98, 177, 178, 207
- Order entry, 107, 108
- Outcomes, 9, 40, 49, 53–55, 57–63, 84, 85, 102, 104, 116, 118, 145–153, 169
 - administration, 134–139
 - business processes, 59–62
 - operations, 139–144
 - OR (Outcome/Raw) data, 94–98, 177, 178
 - use of to define business risks, 133–144, 206, 207
- Outputs, 59–62, 98
- Outsourcing. *See also* Ventoro Offshore 2005 Research Preliminary Findings and Conclusions
 - call centers, 174, 175, 240
 - cost savings from, 13, 14
 - dashboard indicators, 112
 - request for proposal (RFP), 237, 238
 - and risk management, 133, 234–246
 - security guards, 127

- Paper recycling services, 128
- Payroll process, 61, 154, 157, 244, 245

- Period-to-period comparative analysis, 183–187, 209
- Physical mapping
 - administration, 123–125
 - automation, 43
 - creating, 42, 43, 123–133
 - healthcare system example, 43–52
 - IT department, 125–130
 - and key processes, 104
 - modular approach, 172, 173
 - need for, 27
 - operations, 131–133
 - risk registers, embedding, 169–172
- Pick, pack, and stage process, 110, 111, 143, 152
- Pivotal point of change analysis, 179–181
- Proactive approach, 93, 94
- Probability of occurrence, 32, 52, 75, 76, 81–86, 91, 261, 263
- Process chaining, 106–111
- Process owners, 104, 115, 116
- Process-based risk analysis, 75, 76, 101–106
- Production planning and control (PP&C), 108, 109, 140, 143
- Profiling, 190, 192–200, 214, 216–219, 239
- Proprietary data risk, 65, 71, 72, 115, 257
- Purchasing (procurement), 61, 62, 106, 109, 116, 119, 139, 148

- Quality assurance (QA), 142, 151
- Quarry operations, 118, 119

- Ratio analysis, 102, 182, 188, 190, 191
- Real-time risk management, 221–224
- Receiving, 131, 133, 141, 142, 150
- Regulatory compliance, 55, 65, 67, 73, 161–165
- Reporting, 29, 209, 210
- Request for proposal (RFP), 12, 237–239, 255
- Research and development (R&D), 115
- Residual risk, 175, 177
- Return on investment, 22, 138, 148, 249, 262, 266
- Risk analysis for systems environment, 206, 207
- Risk appetite, 28
- Risk assessment
 - attributes of, 81–86
 - banking example, 38, 39
 - business structure as driver of risks, 76, 77
 - components of, 32, 82
 - continuous, 52, 224–226
 - defining risk, 80–91
 - defining the business, 38–40
 - Distributed Risk Assessment and Management (DRAM), 77, 79

- impact analysis. *See* Impact analysis
- multi-dimensional. *See* Multi-Dimensional Risk Assessment
- Multi-Dimensional Risk Assessment, 88–91
- net risk, 175, 177
- probability of occurrence. *See* Probability of occurrence
- process-based, 75, 76
- related risks, 52–57, 62, 63
- residual risk, 175, 177
- risk identification, 82
- root cause analysis. *See* Root cause analysis
- static models for, 3
- Risk categories, 30, 31, 64–74
- Risk chain, 49, 54, 55
- Risk culture, 28, 29
- Risk indicators
 - dashboard indicators, 111–114
 - key early warning indicators (KEWIs), 113, 115
 - Key Process Indicators (KPIs), 30, 59, 88, 98
 - Key Risk Indicators (KRIs). *See* Key Risk Indicators (KRIs)
 - universal risk indicators, 89, 90, 117–120
- Risk language, 28
- Risk management. *See also* ERM (enterprise risk management)
 - ownership, 260, 261
 - proactive versus reactive, 93, 94
 - real time, 221–224
 - stakeholder involvement, 261, 262
- Risk models
 - and ERM, 23–26
 - fluid/dynamic risk model. *See* Fluid/dynamic risk model
 - subjectivity-based, 24–26, 32, 82–86, 94, 99, 174, 175, 266
 - universal risk model, 25, 26
- Risk register, 82, 83, 123, 156–172
- Risk thresholds. *See* Triggers
- Risk universe, 74–76
- Rittenberg, Larry, 4, 15
- Root cause analysis, 42, 76–78, 106, 107, 119, 120, 174, 179–182, 200–202, 226, 227, 256, 261
- Sales and marketing, 107, 139, 148, 149
- SAP, 8
- Sarbanes-Oxley Act (SOX)
 - compliance, 77, 265
 - and COSO framework for internal control, 2, 3, 14–22
 - and fraud, auditing for, 195
 - misconceptions, 1–3
 - private companies, acquisition of, 233, 234
 - violations, 155
- Security guards, 127
- Service level agreements (SLAs), 239–242, 258
- Shareholder value, 219, 220
- Shipping and logistics, 111, 143, 144, 152, 153
- Sources of risk, 36. *See also* Risk categories
- Stakeholders, 40, 261, 262
- Step-down analysis, 181
- Stratification analysis, 119, 120, 186–189
- Subjectivity-based risk models, 24–26, 32, 82–86, 94, 99, 174, 175, 266
- Supply chain management. *See* Purchasing (procurement)
- Systems, Applications & Products in Data Processing (SAP), 8
- Systems design, 205–212, 219
- Systems implementation
 - dynamically integrated risk evaluation (DIRE). *See* Dynamically integrated risk evaluation (DIRE)
 - and future evolution of ERM, 219, 220
 - risk-centric systems, designing, 205–211
 - shortcomings of, 4–13
 - and systems strategies, 204, 205
 - technological risk, 167, 168
 - threshold triggers, 214
- Tax department, 104, 105, 135, 146
- Threshold analysis, 182, 183, 212, 213
- Threshold triggers, 88, 212–215, 265
- Total Quality Management (TQM), 13, 14, 256
- Treadway Commission, 15
- Treasury, 135, 145, 146
- TREC (The Risk Evolution Chain), 53–55, 88
- Trend analysis, 88, 178–180
- Triggers, 88, 212–215, 265
- Union Carbide, 68
- Universal risk indicators, 89, 90, 117–120
- Universal risk model, 25, 26
- Universal risk profiles, 89, 90
- Ventoro Offshore 2005 Research Preliminary Findings and Conclusions, 13, 240, 246–259
- Vona, Leonard, 193
- Wal-Mart, 193
- Wire transfers, 192, 217

<http://www.pbookshop.com>