

Index

• A •

access, 120, 124
access control(s)
 ad hoc approach to, 35
 complicating factors, 118–120
 defined, 25, 117, 321
 described, 115, 116
 mechanisms, 28
 resources, 314
 strategies for cleaning up, 302
accident prevention briefings, 182
accidents, 60, 175–176, 177–182, 186–187
Accor North American, 167
accountability, 72
accounting controls, 321
acid rain program, 204
Adecco SA, 13
ADR legislation in Europe, 229
Advanced Shipping Notice (ASN), 149
Agenda 21, 248
Alcan, 161
Alcoa, 171
American Chemistry Council, 169
American Electric Power, 205
analysis, 121, 135–136
analytics, 262–263
Analyze step, 36
Apple, 224
application security, 272–273
Arthur Andersen, 82, 91
articles as resources, 314, 317,
 318–319, 320
assessing operational risks, 178–179
assessment scenarios, 237
audit(s), 15–17, 321
audit committee, 73, 321
audit compliance, 297
audit fees, 33, 97
audit problems, 16
audit trails, 33, 321
auditability, 262
auditable roles, 122

auditing firms, 22, 32–33, 79
auditors, 113, 129–130
authentication, 116
authorization, 106
Automated Broker Interface (ABI), 145, 149
Automated Commercial Environment
 (ACE), 145
automated controls, 26, 131–133, 138,
 302, 321
Automated Export System (AES), 145
Automated Import System (AIS), 145
automated internal controls, 129
automated risk monitoring, 46–47
automation, 34, 58, 82–83, 261–262, 305

• B •

backup site, 268–269
balanced measurement systems, 249
Barings Bank scandal, 109–110
Basel II, 103, 313, 321
benchmarks, automation yielding, 262–263
benefits for employees, 176–177
best practices, 56, 298, 305–308
Bill 198 (Canada), 16
bill of materials (BOM), 208, 240
board of directors, 44, 73, 321
Boots (company), 224
bottlenecks in global trade, 142
bottom up implementation, 24
brand image, protecting, 255
brand protection, 150
British Petroleum (BP), 252
building materials, 194–196
Bureau of Industry and Security (BIS), 147
business case, 80–81
business partners, 71, 75–76, 150, 277
business planning and innovation, 256–257
business processes, 127–128, 129,
 189–216, 286
business roles, mapping to technical,
 122–123

• C •

- C-11 (Canada), 103, 321
- C-level executives, 47
- C-suite. *See* C-level executives
- CAFTA-DR, 322
- California Climate Registry Voluntary Program, 166
- California Security Breach Information Act, 269
- cap-and-trade systems, 202
- capital, access to, 253
- carbon footprint, 322
- Caremark case, 73
- case management functionality, 292
- CCO (Chief Compliance Officer), 72, 74, 322
- central data repository, 211–212
- central nervous system, 9
- CEO (Chief Executive Officer), 28, 72, 95, 322
- certification of financial reports, 94
- certification process, normalizing, 139
- CFL (ENERGY STAR) bulbs, 168
- CFO (Chief Financial Officer), 10, 28, 95, 322
- change, keeping up with, 271
- change control, 322
- chart of accounts, 322
- checks and balances, 82
- chemical industry, costs of REACH, 233
- chemicals, as hazardous materials, 220–221
- CIO (Chief Information Officer), 98, 322
- cities, going green, 163
- classification, 215, 322
- classifying items for import, 148
- Clause 49 (India), 17, 322
- clean, getting and staying, 121–124
- Clean Air Act, in Canada, 203
- Clean Air Act (CAA), 203–204, 323
- Clean Air for Europe (CAFE), 203
- clean materials and substances, 219
- Clean Water Act (CWA), 204–206, 323
- clearing, customs, 149
- CLERP 9 (Australia), 16, 103, 323
- climate change, 203
- closed-loop system, 37
- COBIT (Control Objectives for Information and Related Technology), 93, 99, 270
- Coca Cola, 92
- code of ethics for financial managers, 94
- collaboration, 232
- Combined Code of Corporate Governance (England), 17
- Commission on Sustainable Development, 249
- common agricultural products (CAP), 155
- communicating, 45, 71
- communications, 228, 280
- companies
 - approaches to GRC, 33
 - going green as, 190
 - green giants, 161
 - image, enhancing, 164–166
 - power and responsibility of, 246–247
 - reasons for going green, 162–163
 - segregation of duties issue, 19
- competition, monitoring changes in, 61
- complexity, 107, 120, 121–123, 146–150
- compliance
 - as the C in GRC, 67
 - continually tracking, 168
 - controls as mechanisms of, 25–27
 - controls ensuring, 24
 - cost of, growing, 33
 - defined, 1, 23–25, 323
 - domains of, 27–30
 - environmental, 169–170
 - global trade guideline concepts, 152–153
 - global trade requiring, 142
 - globalization requirements, 20
 - in GRC, 23
 - initiatives, 12
 - IT GRC in terms of, 269–271
 - as legal side of governance, 68
 - manager cockpit, 236–237
 - managing, 269–270, 274
 - as nonnegotiable, 40
 - process, 25
 - realizing benefits of, 222–225
 - regulations, 236
 - reporting, 226, 237
 - risks, 41
 - system, 79–80
 - violation trends, 74–76
- compliance activities, 12, 27

- Compliance for Products (CfP) application, 236–238
- Compliance Week*, 78, 79, 132
- composite applications, 294
- conferencing technology, securing, 280
- configuration persistence, 289
- construction waste, recycling, 197
- Container Security Initiative (CSI), 147
- Continental Airlines, 161
- continuous monitoring, 137
- control(s)
- automating, 131–133
 - C in GRC standing for, 9
 - as compliance mechanisms, 25–27
 - defined, 1, 25
 - exploring benefits of, 128–131
 - as governance tools, 68, 75
 - in GRC, 23, 293
- control environment, 36, 98, 135–136
- control owners, 127–128
- control testers, 139
- controlled goods, 144, 151
- convergence, 102–103
- COO (Chief Operating Officer), 323
- corporate assets, protecting, 276–280
- corporate governance, 32
- corporate perspective, GRC from, 2
- corporate practices, 107
- corporate procurement policies, 138
- corporations as agents of social change, 252
- corrective controls, 75, 128, 323
- COSO (Committee of Sponsoring Organizations), 93, 98, 99, 270–271, 323
- cost savings from GRC Risk Management, 64
- CPA (Foreign Corrupt Practices Act), 325
- CPM (Corporate Performance Management)
- case for integration with GRC, 284–289
 - defined, 282, 323
 - GRC overlap with, 11
 - integration with GRC in practice, 289–291
 - relationship to GRC, 281–284
- credit checks, 26
- credit ratings, 44, 51
- criminal penalties, 95
- criminal prosecution, 14
- crisis mode, 42
- critical risks, 55
- CRM (Customer Relationship Management), 15, 257, 323
- CRO (Chief Risk Officer), 323
- CSO (Chief Sustainability Officer), 323
- CSR (Corporate Social Responsibility), 245, 253, 255, 256, 258, 324
- CTO (Chief Technology Officer), 322
- culpability, 105
- cultural approach to risk, 46–47
- culture, 47–50, 72
- currency fluctuation, 61
- custody, 106
- customer compliance, 226, 238
- Customer Service component, 187
- customers, shopping green, 253
- Customs Declared Value, 149
- Customs Modernization Act (1993), 153
- customs players, 145
- Customs Trade Partnership Against Terrorism (C-TPAT), 147
- customs value, 324



- dangerous goods, 219, 221–222, 228–229
- dashboards for executives, 285
- data centers, 191
- data formats for compliance data, 236
- Data Governance Institute (DGI), 269
- data privacy, 30, 269, 275–276, 324
- data protection, 278
- decisions, making better, 65
- denied persons list, 20, 324
- detective checks, 135
- detective controls, 26, 75, 128, 324
- DHL, 165–166
- directives, 324
- disaster recovery plan, 268–269
- discharge permits, 205
- disciplines of GRC, 24
- document management, 240, 291
- Document step in SAP GRC process, 36
- documentation, 134
- domains of compliance, 27–30
- DOT (Department of Transportation), 221
- Dow Corning, 234

Dow Jones Sustainability Index, 249
 drayage, 149
 drivers of road vehicles, 229
 dual use of an exported product, 152–153
 due diligence, 237, 271
 Dupont, 231
 duties, 106, 111, 324

● E ●

EAR99, 151
 early warning system, 19
 ECA (European Chemicals Agency), 324
 economic power of corporations, 246
 eCustoms Initiative, 145
 education on workplace safety, 182
 EH&S, 29, 51, 170, 211, 223, 225
 electronic information products (EIPs), 235
 electronic waste, 207
 embargoed country, shipping to, 150, 151
 emissions regulations, 51
 emissions trading, 204, 209, 213, 214
 employee health and safety resources, 316–317
 employees, 173, 174–177, 179, 180, 182, 256
 end-to-end internal controls, 138–139
 end use of exported product, 152
 energy, reducing use and costs, 190–191
 energy consumption, 12
 energy management program, 208–209
 Enron, 82, 91, 92
 enterprise control management, 136
 enterprise risk management, 39–40, 53–57.
 See also risk management
 enterprise-wide initiative, 68
 enterprise-wide solution, 223
 entropy, 105, 111–112
 environment, rising concern about, 12, 170
 environmental, social, and governance (ESG) guidelines, 249
 environmental awareness, 162
 Environmental Protection Use Period (EPUP), 235
 environmental regulations, 20
 environmental risks, 201–202
 environmentalism, 162
 E.ON Energie, 214
 EPA (Environmental Protection Agency), 203–206, 221, 229

ERP (Enterprise Resource Planning), 15, 131–132, 324
 ESG guidelines, 249
 ethical considerations, 256
 EUP (Energy Use in Products), 325
 European Chemicals Agency (ECA), 231
 European Data Protection Directive, 269, 325
 European Social Investment Forum (Eufosif), 253
 events, 117, 166–167
 exceptional access, 120, 124
 exceptions, resolving, 36
 excessive scrutiny, 286
 executives, 49, 72, 251–253
 expectations, unrealistic, 107
 export(s), 141, 142, 325
 Export Administration Regulations (EAR), 147
 export management component, 154
 exporting, 144, 146, 148, 150–153
 exposure, 178, 179
 Exxon, 171

● F ●

facilities, selecting sites for, 192
 failing, audits, 15–17
 failing to comply, 224–225
 fair market value, 325
 FASB (Financial Accounting Standards Board), 93, 325
 Federal Trade Commission (FTC), 325
 Fidelity, 276
 filtered water, 168
 financial close process, 138
 financial compliance, 28, 102–103, 312–313, 325
 Financial Executives International (FEI), 101
 financial information, 14–15
 financial performance, 69
 financial regulations, 14–15, 22, 51
 financial reporting processes, 98
 financial risks, 41, 254, 325
 financials, restating, 101
 flexible work plans, 177
 Flowserve, material weakness, 13
 Foreign Corrupt Practices Act, 102, 150, 313

- fragmented approach to risk management, 43, 45
- framework for governance, 71–76
- fraud
- common examples of, 108–109
 - compared to gross negligence, 111
 - decrease in actions since 2003, 105
 - defined, 106–107, 325
 - at major companies, 11
 - market bubbles as fertile ground for, 91
- FTSE4Good, 249, 253
- **G** ●
- GAAP (Generally Accepted Accounting Principles), 93, 102, 325
- GE (General Electric), 247
- GHG (Green House Gases), 325
- global environmental policy, 195
- global reaction to improving
- governance, 16
- Global Reporting Initiative (GRI), 247, 249
- global trade, 29, 51, 142–147, 152, 153–154, 305–308, 315–316
- global warming, 161
- globalism, 246
- globalization, 20, 141
- going green, 159–160, 161, 164–167, 169–172, 190, 217, 317–319
- Goldman Sachs, 161
- Goodyear Tire & Rubber, 13
- governance
- benefits of good, 69–70
 - defined, 1, 23, 326
 - described, 31, 67–69
 - framework for, 71–82
 - global reaction to improving, 16
 - guidelines, 24
 - relationship to strategy, 290–291
 - structure, 142
- governance office, 70–71
- government
- agencies as GRC stakeholders, 22
 - IT systems, 145
 - links in global trade, 152
 - regulations requiring sustainability, 254
 - report requirements, 61
- GRAS (generally recognized as safe), 218, 326
- GRC Global Trade Services, 62
- GRC (Governance, Risk, and Compliance)
- activities under bailiwick of, 11
 - adoption, 34–35
 - applying too narrowly, 81
 - challenges to comply efficiently, 12
 - cutting costs related to, 19–20
 - defined, 1, 15, 326
 - designing approach to, 33–35
 - goals, 9, 83
 - holistic approach to, 190
 - implementing, 20, 24
 - improvement in, 33, 37
 - integrated approach to, 35
 - integration with CPM, 284–291
 - issues, evaluating, 297–298
 - justifying cost of, 80–81
 - making the most of, 14–20
 - as ongoing investment, 80
 - parts of domain, 10
 - phases of adoption, 33
 - platform, 291–294
 - principles, 133
 - processes, 83
 - program, initiating, 72
 - projects, 300–301, 303
 - resources categorized, 309–310
 - results of, 14
 - reusable technology of, 291–294
 - silos, 79
 - software, 35
 - solutions, 37
 - stakeholders, 20–22
 - strategies, 211, 297–303
 - systems, 28, 35, 36, 85
 - understanding, 9–11, 22–25
- GRC Risk Management Dashboard, 62
- greed as motivation for fraud, 107
- green buildings, 192
- green businesses, 159
- green cleaning, 196–197
- green directives, 223
- green environments, 164
- green facilities, 198
- green legislation, 202–203
- green methodologies, 172, 195
- green practices, 167–168, 195
- green renovation, 196
- greenhouse gases (GHG), 51, 263, 325

Greenpeace, 252
 GRI (Global Reporting Initiative), 326
 gross negligence, 111
 growth, managing, 18–19

• H •

Harmonized Commodity Description and Coding System (HS), 147
 Harmonized Tariff Schedules (HTS), 147, 148, 326
 hazardous materials, 29, 219, 220–221, 225–229
 hazardous substances, 179, 210
 hazardous waste, 215
 hazards, 30–31, 180
 HCS (Hazard Communication Standard), 326
 Health and Safety at Work Act of 1974, 182
 health and safety program, 173, 174, 177–178, 188
 health center, 175, 210
 health of employees, 175
 health risks, selling products with, 254
 health surveillance protocols, 175, 179, 185
 healthcare management program, 184
 healthy benefits, 176–177
 Hewlett-Packard, 161, 164, 276
 HIPAA (Health Insurance Portability and Accountability Act), 275, 326
 historical checks, 135
 HMR (Hazardous Materials Regulations), 227–228, 326
 holistic GRC approach, 83, 190
 Honda, 161
 HVAC, 194

• I •

IASB (International Accounting Standards Board), 326
 IBM, 166, 205, 274
 ICS (Integrated Cargo System), 326
 identity management, 123–124
 identity theft, 30, 275, 326
 IFRS (International Financial Reporting Standards), 93
 implementation plan, 74
 import documents, 145

import license, 326
 import management component, 155
 import restrictions, 327
 importers, 143
 importing, 146, 148–150
 incident, 327
 incident analysis, 57–58
 industrial hygiene and safety, 183, 185–188, 211
 ineffectual controls, 72
 information collected by CPM and GRC, 286
 Information Systems Audit and Control Association (ISACA), 99, 270
 infrastructures, ensuring compliance, 222
 Initial Public Offering (IPO), 17–18
 inspections, 144, 181
 instrumentation of business, 287
 insurance policy, GRC as, 19
 integrated approach, 35, 36, 284–289
 Integrated Cargo System (ICS), 145
 intellectual property, 276–280
 intent, fraud requiring, 107
 interdependence between risks, 55
 Interface, environmental goals of, 247
 interfaces provided by GRC platform, 293
 internal control(s)
 adoption of good, 128
 assessment of, 96–97
 CEO and CFO review of, 95
 COSO's elements of, 98
 defined, 99, 327
 end-to-end, 138–139
 as good governance essence, 127
 implementing, 96
 lack of, 130
 management assessment, J-SOX, 102
 responsibility for, 72
 steps to better, 134–136
 understanding, 127–128
 internal control frameworks, 99, 100
 internal control report, 94, 96
 internal oversight, 82
 internal productivity, 298
 International Civil Aviation Organization, 228
 International Emergency Economic Powers Act (IEEPA), 144–145
 International Financial Reporting Standard (IFRS), 102

International Maritime Organization, 229
 International Traffic in Arms Regulations (ITAR), 146–147
 investors, 12, 21–22, 44, 253
 Investors Financial, 13
 IT
 assets, protecting, 279–280
 frameworks, 99
 making friends with department, 274–275
 modernizing government, 145
 policies, 267
 solutions, 83, 263
 SOX compliance role, 98–100
 speaking with business persons, 119–120
 supporting and managing GRC efforts, 265
 IT governance, 267–271
 IT Governance Institute, 99
 IT GRC, 265–267, 268–269, 315, 327
 items, classifying for import, 148
 ITIL (IT Infrastructure Library), 93, 99, 327

• J •

J-SOX (Japan), 16, 313, 327
 journal entries, 289–290
 jump drive, 278, 279

• K •

Kahoot Products, Inc., 171
 Katrina, 268
 key processes, 28
 key systems, 53
 Kodak, 191
 KonTraG (Act on Control and Transparency in Enterprises) (Germany), 44, 327
 KPIs (key performance indicators), 59, 327
 KPMG, survey, 100
 KRIs (Key Risk Indicators), 59, 64, 65, 327
 Kyoto Protocol, 327

• L •

law, going green as, 169–171
 LEED (Leadership in Energy and Environmental Design), 192, 193, 198–201, 327
 legal and regulatory compliance department, 76, 77–78

legislation, green, 202–203
 legislative bodies as GRC stakeholders, 22
 liability of partners or third-parties, 75–76
 line of business, 49, 50, 51, 327
 litigation, areas of potentially large, 254
 loan processing, automating, 289
 local environments, going green, 163
 log of events, 126
 loss events, 42–43, 57–58

• M •

maintenance notification, 187
 management by exception, 129
 management mentality, GRC as, 13–14
 management oversight in small offices, 123
 management reporting, 283
 managers, 44, 250–251
 manual controls, 26, 27, 139
 manual processes, 35
 manufacturing, 201–207, 208–211
 mapping process, 134
 market, risk of entering new, 60
 Marks & Spencer, 255
 mass exodus, monitoring, 60, 61
 material changes, disclosing, 94
 material master, 215, 238–241
 material weaknesses, 139, 328
 materials, composition of, 219–222
 materials legislation, 229–235
 Mattel, 170–171, 224–225, 246, 261
 MCI, 13
 meta processes, 14
 metrics, measuring energy usage, 208
 Milliken Contract, 167
 mindset changes from internal controls, 131
 mitigating controls, 26, 106, 328
 mobile devices, security for, 279
 Model Regulations on the Transportation of Dangerous Goods, 228
 Molecular Foundry, 199
 monetary value, risk in terms of, 55
 monitored processes, validating, 75
 mop-up operation, 112–113
 motivations for fraud, 107
 MSDS (Material Safety Data Sheet), 211, 228, 240, 328
 multinational corporations, assets of, 246

• N •

NAFTA (North American Free Trade Agreement), 153, 328
 National Commission on Fraudulent Financial Reporting, 99
 National Pollutant Discharge Elimination System (NPDES), 205
 negative, risk as, 48
 negligence, 111, 266, 328
 network, leveraging, 277–278
 New Computerized Transit System (NCTS), 145
 NGOs (non-governmental organizations), 22
 Nike, 246
 NLR (No License Required), 151
 non-hazardous waste, 215
 non-point source pollution, 206
 noncompliance, risks of, 170–171
 Novo Nordisk, 256
 NRC, 221

• O •

objective, 328
 observation of workplace behavior, 178
 obstacles to CPM/GRC integration, 285–286
 occupational health, 183, 210
 Occupational Health module, 184–185
 occupational injuries, costs of, 173
 OCEG (Open Compliance and Ethics Group), 78, 310, 328
 Office of Foreign Asset Control Web site, 152
 Office of U.S. Trade Representative Web site, 152
 ombudsman, position of, 71
 operational risks, 30–31, 41, 328
 opportunities, 30–31, 39–65
 optimization, 36, 136
 orchestrating step in GRC adoption, 34
 order-to-cash business process, 138
 organizations, going green, 163
 OSHA (Occupational Safety and Health Administration), 180, 182, 220–221
 “Our Common Future,” 247
 out-of-the-box monitoring, 137–138

outside scrutiny, inspiring improved GRC, 17

oversight, lack of, 107

ownership, private to public, 17–18

• P •

packing, hazardous materials, 227–228
 Palm, Inc., 224
 paradigm shift for corporate culture, 190
 partners. *See* business partners
 party-level compliance, 144
 password authentication, 116
 passwords, resetting, 123
 pattern recognition technology, 280
 patterns, 106, 178
 PCAOB (Public Company Accounting Oversight Board), 30, 44, 93, 328
 performance and compliance data, 287
 performance indicators, 168
 performance management, 282
 performance metric, 77
 permissions, 117
 Personal Information Privacy Act (Japan), 269, 328
 Personal Information Protection and Electronic Documents Act (Canada), 269, 328
 personnel, shortage of trained GRC, 20
 PG&E, 161
 phrase management, 241
 physical access, 116–117
 planning, 54, 70–71, 282–283
 Plant Maintenance component, 187
 plant maintenance orders, 213
 PLM (Product Lifecycle Management), 15
 point activities, merging, 286
 point source facilities, regulating, 204
 policies, 26, 68, 71, 74, 77
 policy building sessions, 301–302
 policy engine, 292
 political ramifications of scandals, 92
 power crisis, in California, 92
 practices, implementing green, 167–168
 pre-clearance for import, 149
 preregistration process, 232
 preventative checks, 135
 preventative controls, 25, 75, 128, 132

- prevention, achieving total, 184
 prevention principles, 175
 Principles for Responsible Investment, 249
 privacy, 328
 private companies, 18, 104
 private ownership, to public, 17–18
 probability of risks, 55
 problems discovered by controls, 27
 procedures, 68
 process control, 314, 329
 process modeling, 292
 processes, 74, 190, 202
 procure-to-pay process, 132, 138
 product compliance, benefits of, 223–224
 product-level compliance, 144
 product safety, ensuring, 211
 product values, reconciling, 149
 production plants, evaluating, 62–63
 products, 152–153, 217–241
 profits, CRS increases, 257
 program management, 32
 progression of GRC adoption, 34
 prohibited companies, 10
 Project Big Green, 166
 public ownership, 17–18
 public trust, decline of, 91
 pure substances, 219
- **Q** •
- Quality Management component, 187
 quantifying risks, 55
 Qwest, 92
- **R** •
- REACH (Registration, Evaluation and Authorization of Chemicals)
 described, 147, 230–234, 329
 guidelines, 254
 real-time checks, 135
 real-time monitoring, 129–130
 reasonable care of exported items, 153
 reconcile to report business process, 138
 reconciliation, 106, 149
 record keeping, 106
 recruitment retention, 176–177
 recycling, benefits of, 197–198
 reduction, cost, 19–20
 Reduction of Hazardous Substances (RoHS), 206
 refrigerants, green, 194
 Regional Greenhouse Gas Initiative (RGGI), 202
 regulators, concern about risk, 44
 regulatory authorities, building trust with, 166
 regulatory risks, diversity of, 51
 Remediate step, 36
 remediation, 135, 139
 renovation, green, 196
 reporting and consolidation phase, 283
 reporting in GRC platform, 293
 reporting process for sustainability, 259
 reporting requirements after failed audit, 16
 repository on GRC platform, 291
 residents, going green, 163
 resource availability, 298
 response process to risks, 56
 responsibilities, 45, 110, 135
 restatement, 329
 restitution management component, 155
 restricted parties lists, 144, 150
 reticence about risk, 48
 revenue leakage, 138
 RFID (Radio Frequency Identification) tags, 279
 Rio Declaration on Environment and Development, 248
 risk(s)
 approaches to handling, 42
 assessing, 178–179
 defined, 1, 23, 40–41, 329
 evaluating responses to, 42
 identifying and analyzing, 55
 ignoring, 42–43
 managing, 19
 of noncompliance, 170–171
 prioritized and mitigating, 31
 as the R of GRC, 67
 regulatory, 51
 reticence about, 48
 stakeholders' concern about, 44
 systematic monitoring of, 43
 risk analysis, 329

- risk appetite, 59, 329
 - risk assessment, 54, 98, 177, 185–186, 201
 - risk avoidance, 55
 - risk dashboards, 57
 - risk expertise, leveraging, 51
 - risk identification and analysis, 53, 55
 - risk management
 - approaches to, 43–47
 - as competitive advantage to SAP, 64
 - compliance, 29
 - consolidating with strategy, 65
 - cycle, automating, 58
 - defined, 30
 - framework for, 47–53, 329
 - new approach to, 39
 - organization, 50–52
 - process, 54, 76–77
 - program, 42
 - protecting and creating value, 40
 - resources, 311–312
 - results of, 24
 - strategy, 270
 - risk managers, 45, 49, 50–52
 - risk mitigation, 329
 - risk monitoring, 54, 56–57
 - risk planning, 54
 - risk policy, 47
 - risk response, 53, 55–56, 329
 - RoHS (Reduction of Hazardous Substances), 224, 234–235, 329
 - role cleanup, aggregating, 303
 - roles
 - analyzing, 112
 - assigned to computer system users, 28
 - defined, 117
 - escalation in number of, 118–119
 - one or more for each user, 115
 - proliferation of unique, 107
 - scanning existing, 125
 - rule engine, 293
 - rules, playing by, 25–30
 - rush to clean up, 33–34
 - rush to comply after SOX, 10
- S ●
- safe work practices, rewarding, 176
 - safety measures, 181
 - safety program, 183
 - safety risks, 175
 - sampling, 129–130, 133
 - sanctioned party lists, 51
 - SAP, 2, 83, 195, 235–241
 - SAP Customer Relationship Management, 60, 61
 - SAP Environment, Health & Safety, 60, 184–188, 238–241
 - SAP Environmental Compliance, 212–214
 - SAP ERP, 60, 61
 - SAP ERP Human Capital Management, 185, 188
 - SAP Financial, 213
 - SAP GRC Access Control, 125–126
 - SAP GRC Global Trade Services, 84, 154–155
 - SAP GRC Process Control, 36, 136–139
 - SAP GRC Repository, 83–85, 136–137
 - SAP GRC Risk Management, 58–65, 84
 - SAP Human Capital Management, 60
 - SAP NetWeaver, 187, 236
 - SAP Product Lifecycle Management, 213
 - SAP Project System, 60
 - SC Johnson, 161
 - SCM (Supply Chain Management), 15, 329
 - scrutiny, inspiring GRC performance, 17
 - searches for specifications, 241
 - SEC (Securities and Exchange Commission), 30, 44, 93, 254, 329
 - Securities Act (1933), 91
 - security compliance, 30
 - security for software applications, 272–275
 - security initiatives, 144–145
 - segregation of duties (SoD), 11, 19, 25, 75, 106, 121, 125, 297, 330
 - self-governance, 31–32
 - self-inflicted rules, 25
 - separation of powers, 106
 - shareholder, 69, 330
 - Shell UK, 252
 - shipping cut-offs, improper, 138
 - sick building syndrome (SBS), 198, 330
 - SIEF (Substance Information Exchange Forum), 232, 330
 - siload approach to risk management, 45
 - silos, avoiding GRC, 79
 - SIMEX (Singapore International Monetary Exchange), 109, 110
 - single system of record, 136–137

- site plan, green principles for, 193
 - Site Specific Targeting Program, 180
 - sites, 181, 187, 192
 - Socially Responsible Investors (SRI), 253
 - Societe Generale, 130
 - sociopolitical compliance, 10
 - software applications, securing, 272–275
 - Sony, 224
 - SOX (Sarbanes-Oxley Act)
 - applicability of, 90
 - basics of, 93–97
 - benefits of, 103–104
 - costs of, 100–101
 - described, 89, 330
 - environmental liabilities and risks, 254
 - impact on global trade regulation, 147
 - necessity for, 91–92
 - placing of responsibility and
 - accountability, 72
 - regulations introduced by, 28
 - resources, 312
 - rush to comply with, 33–34
 - Section 302, 14, 28, 93–96
 - Section 401, 94
 - Section 404, 94, 96–97
 - Section 406, 94
 - Section 409, 94
 - Section 802, 94
 - Section 906, 94, 95
 - specification information system, 241
 - spreadsheets, shortcomings of, 236
 - stakeholders, 20–22, 44, 247, 251–253, 330
 - standard operating procedures, 179, 186
 - state air pollution agencies, 203
 - statistical evaluation of accident data, 187
 - status of a risk, 56
 - statutory reporting, 283–284
 - stewards for goods, 229
 - stock market bubble, 91
 - stock price declines due to loss events, 42
 - strategic initiatives, 74, 80
 - strategic resource allocation, 282
 - strategic risks, 41, 330
 - strategies, 283, 290, 297–303
 - strategy management, 65, 282
 - substance database, 186
 - substance volume tracking, 240
 - substances, 219, 230, 330
 - success, 41, 299
 - Sun Microsystems, 165
 - Suncor, 161
 - superusers, 112, 117, 124
 - supervision, lack of, 110
 - supplier compliance management, 226, 237–238
 - supplier concentration, 288
 - supplier reliability, 60
 - suppliers, tracking, 277
 - supply chains, 143–144, 147, 233, 261–262, 330
 - sustainability
 - as business strategy, 246
 - confusion about meaning of, 258
 - defined, 245, 247–248, 330
 - as good business, 250–257
 - managing performance, 258–260
 - reporting, 30, 259, 260–263
 - resources, 319–320
 - resulting from good governance, 69
 - sustainable resources and materials, 192–198
 - SVHC (Substances of Very High Concern), 233, 330
 - Swiss Re, 161
 - Switzerland, 29, 44
 - system of record, 330
 - system permissions, 112
 - systematic approach to risk, 45–46
 - systematic framework for site management, 52
- T ●
- tactical issues, compliance and risk as, 79
 - tactics, 74
 - task management, comprehensive, 226–227
 - tax credits for LEED certification, 200–201
 - technical and business issues,
 - separating, 302
 - technical roles, 122–123
 - technology, exploiting, 194
 - technology infrastructure, 52–53
 - teleconference solutions, 198
 - temporary IDs, issuing with expiration, 126
 - temporary users, 112
 - terrorist attacks, 11
 - Tesco, 161
 - Test step in GRC process, 36

testing, 135
 theft from company, 109
 threat modeling, 272–273
 thresholds, 25, 59
 Timberland, 165
 TLAs (Three-Letter Acronyms), 15
 top-down structure for GRC, 24
 Toxic Release Inventory, 230
 Toxic Substances Control Act (TSCA),
 179, 229–230, 330
 Toyota, 196, 247
 tracking of virtual things, 119
 trade management, 28–29
 trade organizations as GRC
 stakeholders, 22
 trade preference management, 153, 155
 training, assessing, 77
 transactions, 27, 117
 transparency, 93, 330
 travel, reducing, 198
 trees, planting, 167
 tremcards, 228, 229
 triple bottom line, 245, 250, 259
 trust, building with regulatory
 authorities, 166
 Tyco, 92

• U •

uncertainty, 47
 Union Carbide, 171
 United Nations, sustainability
 indicators, 30
 unmanaged risks, 31
 unrealistic expectations, 107
 U.S. Amended Sentencing Guidelines, 29, 44
 U.S. Climate Action Partnership (USCAP),
 166, 167
 U.S. Customs, 145, 149, 152
 U.S. Green Building Council, 192, 193

U.S. Voluntary Reporting of Greenhouse
 Gases Program, 166
 user provisioning, 124, 126
 users, 112, 117, 118–119, 120

• V •

value chain sustainability application, 262
 vehicles, transporting hazardous
 materials, 228
 vendor MSDSs, 228
 venture capitalists, 253
 videoconferencing, 198
 virtual things, tracking, 119
 visibility, increased, 64

• W •

Wal-Mart, 149, 164–165, 248, 262
 warning signs, watching for, 110
 waste management, centralizing, 210
 Waste Management module, 212, 215–216
 watch lists, 51
 water, 168, 194, 205
 waterless urinals, 194
 WEEE (Waste Electrical and Electronic
 Equipment), 206–207, 330
 Western Governor's Association
 (WGA), 202
 what-if scenarios, 65
 whistle-blowers, 90
 wikis, 314, 318
 work plans, flexible, 177
 workflow provided by GRC, 292
 working environment, 61
 workplace, 177, 182
 World Commission on Environment and
 Development, 247
 WorldCom, 92