

# Index

## A

accounting scandals, 9, 83  
accounts payable questionnaire,  
111–13  
agreements, labor, 39  
American Institute of Certified Public  
Accountants, 163  
analytical and consultative services,  
123  
application controls, 44  
approval matrix, 72–73  
approval policy and procedures, 69–73  
audit committee, 7, 54, 56, 60, 91–92,  
145–48  
Auditing Standard No. 2, 144  
Auditing Standard No. 5, 84  
Auditing Standards Board  
Risk Assessment SASs (SAS 104–111),  
4–5, 8  
Statement of Auditing Standards (SAS  
115), 4, 8–9, 26  
Audit of Financial Statements, 144  
auditor attestation, 132  
*AU Section 316, Consideration of Fraud in  
a Financial Statement Audit*, 82–83,  
114–19  
authority and responsibility, 33–34,  
59–60  
automation, 149–55, 159, 161

## B

best practices, 140–42, 145  
board of directors  
activities, 55

COSO and, 55–57  
ERM duties and responsibilities,  
21, 23  
ERM-Integrated Framework, 33  
executive compensation, 61  
fiduciary responsibility and  
accountability, 18  
IFRS initiatives, 166  
opinion survey, 91  
oversight and stewardship, 18  
risk management, 5, 7, 17–19, 36  
BPM. *See* business performance  
management (BPM)  
brand, 29–30  
business  
process improvement/automation,  
140  
requirements, defining, 160  
risk, 2, 7–8, 145  
business performance management  
(BPM), 122, 140

## C

capital allocation, 13, 39  
certification issues, 150  
CFO. *See* chief financial officer (CFO)  
*CFO Magazine*, 10  
change management protocols, 39  
chief auditors, 122  
chief executive officer (CEO), 21–22,  
121  
chief financial officer (CFO), 121, 147  
code of ethics, 20, 54, 57, 63–66, 121  
collusion, 48

Committee of Sponsoring Organizations (COSO), 3

- authority and responsibility, 59–60
- board of directors, 55–57
- control environment, 52–53, 90–95
- deficiencies, evaluating, 86
- entry level controls, 83–84
- ERM—Integrated Framework*, 4, 25, 28, 31–34, 76
- financial controls, 49–52
- financial reporting competencies, 58–59
- financial reporting objectives, 75–76
- financial reporting risks, 76–77
- Framework, five components of, 51
- fraud risk, 77–83
- human resources, 60–61
- integrity and ethical values, 53–55
- internal control, defined, 4, 51, 58
- internal control evaluations, 89
- Internal Control—Integrated Framework*, 51
- Internal Control over Financial Reporting*, 53, 55, 57, 59–60, 75, 77, 86
- management philosophy and operating style, 57
- organizational structure, 57–58
- oversight, 47
- risk assessment, 74–75
- risk assessment and financial controls example, 84–85
- top-down risk-based approach, 52
- communication, 45–46, 101–3
  - information and, 27–28
- compensation schemes, 165
- competence commitment, 34
- completeness, 75
- compliance
  - monitoring, 149, 151, 156
  - objectives, 37–38
  - optimization, 133–34
  - optimizing, 133–38
  - plan, ongoing, 138–39
  - software, 151–52
- component depreciation, 164
- computer controls, 44

- confidential information, 65–66
- conflict of interest, 64–65
- Consumer Protection Act (2010), 9
- continuous monitoring
  - benefits of, 154–55
  - process, 155–57
  - tool considerations, 155
- control
  - activities, 27, 43–44, 85, 99–100
  - automation, 142, 153–55
  - environment, 52–53, 90–95
  - improvements, 128
  - self-assessment questionnaire, 77
  - testing, 141–42, 149, 151, 153–54, 157, 159–60
- corporate culture, 19–20
- Corporate Executive Board, 10
- corporate governance, 17, 23, 127, 131, 134, 147
- corporate scandals, 7, 18
- COSO. *See* Committee of Sponsoring Organizations (COSO)
- credit/cash management, 30
- criminal penalties and fines, 121
- cultural and language barriers, 166
- customer satisfaction/dissatisfaction, 39

## D

- data, 155–56
- debt and equity structure, 30
- debt covenants, 166
- Department of Labor, 31
- designated approver, 70
- disclosure, 133, 136, 139, 142, 144
- dividend policy, 166
- Dodd-Frank Wall Street Reform, 9
- downside risk, 11–12

## E

- economic factors, 38
- employee empowerment, 60
- Enron, 9, 18, 83
- enterprise risk management (ERM)
  - activities of, 26–27
  - benefits of, 12–13
  - board of directors, 21
  - business case for, 11–13

- communication, 45–46
  - compliance plan, 140
  - components of, eight, 27–28
  - control activities, 43–45
  - definition, 1, 7, 25–28
  - design and implementation, 35–47
  - event identification, 38–40
  - executive support, 13
  - external events, 38–39
  - frameworks and standards, 3
  - informal, 2, 8
  - information controls, 44
  - internal audit, 23
  - internal factors, 39
  - management, 21–22
  - objectives, 28
  - in organizational view, 6
  - oversight, 47
  - policies and procedures, 44
  - publications, 3
  - requirements, 135
  - risk and strategy, 14
  - risk and uncertainties, 7
  - risk assessment, 40–42
  - risk effects, 26
  - risk monitoring, 46–47
  - risk officer, 22–23
  - risk response, 41–43
  - risks, high, 15
  - roles and responsibilities, 20–23
  - strategy and objective definition, 36–38
  - success, keys to, 13–15
  - top-down monitoring, 17–18
  - enterprise strategy, 123
  - entity-level control, 74, 77, 83–84, 88–110
  - entry level controls, 83–84
  - equity as debt, reclassifying, 166
  - ERM. *See* enterprise risk management (ERM)
  - ERM—*Integrated Framework*, 4, 25, 28, 31–34, 76
  - ethical behavior, 20, 54–55, 133
  - ethical standards, 120, 124, 134
  - European Commission, 162
  - event identification, 27, 38–40, 84
  - exception remediation, 156–57
  - executive compensation, 61
  - executive management, 5, 7, 92–94, 121, 124, 166
  - executives, 90–91
  - external communication, 46
  - external risks, 30
- F**
- false-positive minimization, 155
  - finance strategy, 123
  - financial
    - close, 136, 159
    - controls, 49–52
    - restatements, 133, 142
    - risks, 30
    - statement, 53, 85
  - financial reporting
    - about, 3, 30, 50, 127–28
    - competencies, 58–59
    - misstatements, 61
    - objectives, 75–76, 84
    - positions, 60
    - risks, 76–77
  - Foreign Corrupt Practices Act*, 70
  - fraud, 7–10, 82
    - policies and procedures, 82
    - risk, 77–83, 114–19
  - fraudulent
    - activities, 39
    - financial reporting, 3, 82–83
    - transactions, 39
  - FTEs. *See* full-time employees (FTEs)
  - full-time employees (FTEs), 142
  - functional activity management, 43
- G**
- generally accepted accounting principles (GAAP), 163–65, 167
- H**
- high-risk incidents, 35
  - human resources, 60–61, 95
- I**
- IASB. *See* International Accounting Standards Board (IASB)

IFRS. *See* International Financial Reporting Standards (IFRS)

impairment reversal, 165

information, 31, 43

risks, 101–2

technology controls, 136

information technology (IT), 165, 171

infrastructure, 39

insider trading, 121

integrated risk, 3

integrity and ethical values, 33, 53–55

intellectual property, 65–66

interest rate fluctuations, 30

internal audit, 23, 143–44

internal control, 8

assessment, 112–13

concepts, 87

deficiency in, 86

defined, 4, 51, 58

entity level survey, 88–110

evaluations, 89

of financial reporting, 50, 121

monitoring survey, 105–8

testing, 132–33

internal environment, 27, 31–34

Internal Revenue Service, 31

International Accounting Standards

Board (IASB), 163, 167–68

*International Financial Reporting for Small and Medium-sized Entities* (SMEs), 163

International Financial Reporting Standards (IFRS), 162–72

## L

last-in-first-out method of accounting, 164

## M

management

ERM duties and responsibilities, 21–24

override, 48, 85

philosophy and operating style, 57

material

misstatement, 77, 84–86

weakness, 86

materiality concept, 75

metrics, key performance, 166

misappropriation of assets, 82–83

misstatements, 150

mitigation, 2

monitoring, 28, 105–8

monitoring software, 152–53

## N

natural environment, 39

New York Stock Exchange, 18

nonaccelerated filers, 132–33

## O

objective setting, 27

Occupational Safety and Health Administration, 31

operational risks, 30–31

operations objectives, 37

organizational structure, 33, 57–58, 93–94, 121, 126

outsourced functions, 137

outsourcing, 39, 141

overall risk, 49–50, 52

## P

PCAOB. *See* Public Company Accounting Oversight Board (PCAOB)

performance indicators, 43

period-end financial results, 85

personnel, 39, 137

physical controls, 43

political events, 39

postmerger integration, 136–37

presentation and disclosure, 75

process

change procedure, 127

documentation, 40

execution errors, 39

improvement, 122–23, 125–29, 131

level control, 52

modification, 39

procure to pay process flow, 80–81

production stoppages, 39

productivity improvements, 128

Public Company Accounting Oversight Board (PCAOB), 4, 88–89

purchasing controls questionnaire,  
111–12

## R

record retention, 121

regulatory guidance, 7

regulatory risks, 31

related party transactions, 70

remediation

about, 76, 133, 137, 139, 143, 146

prioritization, 127–29

reporting automation, 149, 151

reporting objectives, 37

reputation, 30

reputational damage, 39

reevaluation, 165

rights and obligations, 75

risk

acceptance, 29

appetite, 28–29, 33, 35, 38

assessment standards, 8

avoidance, 29

categories, 30–31

control matrix, 78

governance, 17

identification, 2

incidents, 35

intelligent culture, 13–14

limits, 29

management philosophy, 32–33

management software, 157–58

management technology, 158

mitigation, 5, 7, 20, 29, 50

monitoring, 46–47

of noncompliance, 132, 161

officer, 22–23

profile, 1, 3, 35

thresholds, 8

tolerance, 23, 29

transfer, 29–30

transparency, 12

risk assessment, 27

aggregate entity consequences in, 2

compliance with laws and regulations,

6

control activities in place, 99–100

of control environment, 138

COSO and, 74–75

defined, 74

ERM and, 40–42

event identification and, 84

managing change, 97–98

objectives, company-level, 96

objectives, process-level, 97

policies and procedures, 99

process, 2, 6

risk identification, 97

risks identified by control activities, 6

stakeholder value and uncertainty, 2

survey, 96–98

risk management, 8

barriers, perceived, 11

business processes, 3

centralized, 3

corporate governance, 17, 23

deficiencies in, 47

defined, 1

importance and benefits, 2

as offensive weapon for management,

3

organizational view of, 134

organization view of, 5–6

pressure for, 8–9

risks in multiple business areas, 2

“silos,” 2, 12

risk response, 41–43, 46, 85

categorization of, 36

definition, 29–30

ERM process, 27, 35–36, 40–44, 46

## S

Sarbanes-Oxley Act (SOX), 4, 31, 50

centralization/standardization, 130

compliance, generating value from,

121–23

compliance, moving beyond initial,

123–25

compliance, ongoing, 125–27

compliance, optimizing, 136–38

compliance and financial reporting,

128

compliance optimization process, 135

- Sarbanes-Oxley Act (SOX) (*Continued*)
- compliance plan, ongoing, 138–39
  - compliance program, reevaluating, 125–27
  - control improvements, 128
  - costs and time for compliance, 121
  - criminal penalties and fines, 121
  - decentralization/customization, 130
  - ERM strategy and, 122
  - internal controls, 88
  - operational structure and efficiency, 129–30
  - origins of, 120–21
  - prioritization on business impact and complexity, 129
  - process improvement, 129
  - productivity improvements, 128
  - remediation prioritization, 127–29
  - Section 302, 121, 124, 126–27
  - Section 404, 5, 76–77, 88, 121, 123–24, 126–27, 129–30, 132, 139, 143–44
  - Section 409 — Real Time Issuer Disclosures, 126
  - transparency of financial reports, 162
- SAS 115, *Communicating Internal Control Related Matters Identified in an Audit*, 8–9, 86
- SEC. *See* Securities and Exchange Commission (SEC)
- Securities Acts of 1933, 120
- Securities Acts of 1934, 70, 120
- Securities and Exchange Commission (SEC)
- about, 4, 31, 77, 121
  - COSO Framework, 51
  - IFRS roadmap, 163
  - risks, information on, 9–10
  - top-down risk approach, 4
  - security breaches, 39
  - segmental reporting, 164, 166
  - segregation of duties, 43
  - senior management team, 12, 43, 53
  - significant deficiency, 86
  - single-exception identification, 155
  - SMEs. *See International Financial Reporting for Small and Medium-sized Entities (SMEs)*
  - social events, 39
  - software vendors, 153, 160
  - SOX. *See* Sarbanes-Oxley Act (SOX)
  - Statement of Auditing Standards 70 type II letter, 137
  - strategic risks, 31
  - systems downtime, 39
- T**
- technological events, 39
  - technology leverage, 123
  - transaction processes, supporting, 50
  - transparency, 120, 162, 167–68
  - Treadway Commission, 3, 25, 51, 74, 89
- U**
- unethical activity, suspected, 54–55
  - upside risk, 11–12
  - U.S. “nonissuers,” 163
- V**
- valuation or allocation, 75
  - value creation, 17
  - vendor candidates, identifying, 160
- W**
- whistleblower, 20, 54, 57, 67–68, 121
  - workplace accidents, 39
  - WorldCom, 9