

INDEX

A

Accounting changes, 11
Accounting manuals, 122–123
Activities, control:
 in COSO framework, 30, 38–40
 and small business, 46
Activities, internal audit, 89–90
Activity-level controls, 16–17, 75–76,
 208–233
 design effectiveness of, 211–214
 documentation of, 123–147,
 234–235
 evaluation of, 158
 example inquiries, 236–237
 objectives for, 79
 operating effectiveness of, 214–231
 tests of, 214–233
 walk-through to check, 209–211
Annual reporting requirements, and
 evaluation of control deficiencies,
 245–249
Anti-fraud programs/controls:
 control objectives for, 78, 163
 and project scoping, 67–69
Applications, computer, 180
Application-level controls:
 and entity-level controls, 168–170
 general controls vs., 178
“As of” criterion, 246–249
Assertions, financial statement, 212,
 213
Assignment of authority and
 responsibility, 34
Attitudes, assessing employee,
 199–200

Audits, improved effectiveness of, 20
Audit committee, 58–60, 69
Auditors, independent, *see*
 Independent auditors
Authority, assignment of, 34

B

Beliefs, shared, 55–56
Board of directors, 59
Board of directors’ charter, 119

C

Carter, M., 57
Cell phone usage, reimbursement
 for, 6
Center for the Study of Ethics in the
 Professions, 166*n*.2
CEO, *see* Chief executive officer
CFO (chief financial officer), 100
Change(s):
 in documentation, 152
 misstatement risk and managing,
 10–11
Chief executive officer (CEO), 30, 34,
 59, 100
Chief financial officer (CFO), 100
COBIT framework, *see* Control
 Objectives for Information
 and related Technology
 framework
Code of conduct, written, 119–120
Collusion, 28
Commitment to competence, 33

- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report, 2, 11, 26–51, 54, 83, 168
- background of, 26–27
- business objective-driven approach in, 28–29
- control activities discussed in, 38–40
- and control environment, 31–35
- and corporate culture, 56
- and creating of optional internal reports, 249–250
- five essential components of internal control in, 30–31
- flexible approach in, 29
- holistic/integrated approach in, 27–28
- and human element, 29–30
- information/communication system discussed in, 41–44
- and information technology systems, 48–51
- and internal control as process, 28
- and reasonable assurance principle, 29
- and risk assessment, 35–38
- small business, applicability to, 44–48
- Communication(s):
- in COSO framework, 28, 30
 - formal vs. informal, 42–43
 - and small business, 47
- Communication systems, 41–44
- Compensating controls, 243
- Competence:
- of auditors, 22
 - management’s commitment to, 33
- Completeness (financial statement assertion), 213
- Computer application controls, 131
- Confidence level, 222
- Controls:
- activity-level, 16–17. *See also* Activity-level controls
 - in COSO framework, 27
 - documenting evidence related to testing of, 7
 - entity-level, 16, 19. *See also* Entity-level controls
 - evaluating operating effectiveness of, 7
 - identifying, 7
 - redundant, 17
- Control deficiencies, 4, 238–253
- and annual/quarterly reporting requirements, 245–249
 - and compensating controls, 243
 - and coordination with independent auditors, 252–253
 - and coordination with legal counsel, 253
 - defining, 83–85
 - design vs. operating deficiencies, 229
 - evaluation of, 239–245
 - improved remediation of, 19
 - and management’s responsibility for internal control, 249–252
 - as material weaknesses, 241–243
 - origins of, 239
 - and possibility of misstatement, 240–241
 - and “prudent official” test, 243–245
 - reporting of, 44
- Control failure:
- likelihood of, 14–15
 - risk of, 5
- Control objectives:
- example, 77–79
 - identification of significant, 75–76
- Control Objectives for Information and related Technology (COBIT) framework, 26, 48–51
- Corporate culture:
- control objectives for, 77, 160–161
 - and project scoping, 55–57, 68
- Corporate governance documents, 118–121
- board of directors’ charter, 119

- code of conduct, 119–120
 - disclosure committee charter, 121
 - Corporate restructurings, 11
 - Corrective actions:
 - with entity-level controls, 188–189, 197, 199, 200
 - of operating deficiencies, 246–249
 - COSO framework, 151
 - COSO Report, *see* Committee of Sponsoring Organizations of the Treadway Commission Report
 - Criteria for internal control, 25–51
 - and COSO integrated framework, 26–40
 - information and communication as, 41–44
 - need for, 26
 - for small business, 44–48
 - with technology systems, 48–51
 - Critical success factors, 35
 - Culture, corporate, *see* Corporate culture
- D**
- Databases, 180
 - Deficiencies, *see* Control deficiencies
 - Design:
 - deficiencies in, 235
 - of entity-level controls, 170
 - Detective controls, 17, 130
 - Disclosure (financial statement assertion), 213
 - Disclosure committee, 90–91
 - Disclosure committee charter, 121
 - Documentation, 23, 115–156
 - accounting manuals, 122–123
 - action plans for, 157–159, 234–235
 - of activity-level controls, 123–147
 - adequacy of existing, 116–118
 - assessment of existing, 157–158
 - content considerations, 126–127
 - and control objectives, 160–166
 - and coordination with independent auditors, 156, 159
 - corporate governance documents, 118–121
 - design of, 124–127
 - of entity-level control
 - policies/procedures, 118–123
 - flowcharting as method of, 127–136
 - human resource policies and personnel handbook, 121–122
 - importance of, 115–116
 - matrixes as method of, 141–147
 - narratives as method of, 137–141
 - of planning decisions, 105–106
 - and Sarbanes-Oxley automated compliance tools, 147–155
 - techniques of, 125
 - of tests of activity-level controls, 232
 - of tests of entity-level controls, 190
- Duties, segregation of, 40
- E**
- Effectiveness, of entity-level controls, 185–190
 - EITF (Emerging Issues Task Force), 92
 - Embezzlement, 13
 - Emerging Issues Task Force (EITF), 92
 - Employees:
 - reimbursement of, for cell phone usage, 6
 - surveys of, 171–176, 194–200
 - Employee qualifications, 227
 - Enterprise Risk Management Framework*, 51n.1
 - Entity-level controls, 16, 19, 167–191
 - and application-level controls, 168–170
 - and coordination with independent auditors, 190–191
 - and design vs. operational effectiveness, 170
 - documentation of, 118–123

- Entity-level controls (*contd.*)
 and documentation of test results, 190
 effectiveness of, 185–190
 evaluation of, 158, 185–190
 objectives of, 75
 overall objective of, 167–168
 testing techniques for, 170–185, 192–193
- Environment, control, 31–35
 and assignment of
 authority/responsibility, 34
 and commitment to competence, 33
 in COSO framework, 30
 and ethical values/integrity, 31–33
 and human resource
 policies/practices, 34–35
 and management's
 philosophy/operating style, 33
 and organizational structure, 33–34
 and small business, 46
- Error, human, 28
- Error rates, 222
- Ethics, culture of, 68
- Ethical values:
 and control environment, 31–33
 in employee survey, 198, 199
- Evaluation, of control deficiencies, 239–245
- Evaluation of internal control:
 by management, 1–4
 and risk-based judgments, 4–7
 top-down approach to, 8–23
 and use of independent auditors, 23–24
- Events, transactions vs., in flowcharts, 129–130
- Existence (financial statement assertion), 213
- Existing documentation, assessing
 adequacy of, 116–118, 157–158
 and deciding what to document, 117
 and scope of documentation, 117–118
- Explicit assertions (in financial statements), 212
- F**
- Failure, control, *see* Control failure
- Finance officers, control-related responsibility of, 59
- Financial information:
 and IT general controls, 62
 monitoring of, 67
- Financial statements:
 assertions of, 212
 and entity-level controls, 171
 and IT general controls, 61
- Flexible approach, 29
- Flowcharting, 127–136
 benefits of using, 127
 and computer application controls, 131
 drawbacks of using, 128
 example of, 131–136
 and flow of information, 128
 and information storage/retrieval, 130–131
 and preventive vs. detective controls, 130
 and system boundaries, 128–129
 tips for, 128–131
 and transactions vs. events, 129–130
- Focus groups, 223–231
 conducting, 227–229
 confirming control design for, 224–226
 and employee qualifications, 227
 and facilitation of group discussions, 229
 and identification of exceptions, 226–227
- Follow-up, 40
- Foreign operations, 11
- Form 10K, 2, 93–99
- Form 10-Q, 247

Formal communications, 42–43

Fraud:

anti-fraud programs/controls, 67–69

and project scoping, 67–69

Fraud risk, 12–13

G

GAAP, *see* Generally accepted accounting principles

General controls, application controls vs., 178

Generally accepted accounting principles (GAAP), 8, 11, 37, 72, 97

H

Holistic/integrated approach (in COSO Report), 27–28

Honesty, culture of, 68

Human element, 29–30

Human error, 28

Human resource policies, 121–122
and control environment, 34–35
and culture of honesty/ethics, 68

I

Implicit assertions (in financial statements), 212

Incentives:

and ethical values, 32

for fraud, 13

Independent auditors, 20–23

and control deficiencies, 252–253

documentation and coordination with, 156, 159

overall objective of engagement of, 20

and project planning, 103–105

and testing/evaluation of entity-level controls, 190–191

and tests of activity-level controls, 232–233

using work of, 21–23

working with, 23–24

Informal communications, 42–43

Information:

in COSO framework, 28, 30

flowcharting and storage/retrieval of, 130–131

flow of, in flowcharts, 128

gathering of, in project planning stage, 82–93

integrity of, 151–152

routine vs. nonroutine, 42

and small business, 47

sources of, in project planning stage, 93–99

Information processing, 40

Information-processing streams, 212–214

Information systems, 11, 41–44

Information Systems Audit and Control Association (ISACA), 26, 48, 103

Information technology (IT), 26, 51

application controls, 216–217

control objectives for, 77–78, 162

general controls for, 178–181

and project scoping, 60–62

Information Technology Governance Institute (ITGI), 103

Information technology systems, 48–51

Inquiries, 99, 176–178, 201–206. *See* also Focus groups

Integrity:

and control environment, 31–33

information, 151–152

Interest rates, 9

Internal auditors, control-related responsibility of, 59

Internal control, 2

Internal control criteria, *see* Criteria for internal control

Internal Control–Integrated Framework, 26, 44

Intervention, by management, 33

Inventory counts, 5
 ISACA, *see* Information Systems
 Audit and Control Association
 IT, *see* Information technology
 ITGI (Information Technology
 Governance Institute), 103

J

Judgments, risk-based, 4–7

K

Krispy Kreme Doughnuts, Inc., 98–99

L

Lambert, M., 57
 Legal counsel, coordination with, 253
 Locations, company, 85–86

M

Management:
 control-related responsibility of, 59
 evaluation of internal control by,
 1–4
 and importance of understanding
 risk, 6–7
 inquiries of, 176–178, 201–206
 intervention of, and ethical values,
 33
 objective of, 3
 philosophy/operating style of, 33
 responsibility of, for internal
 control, 249–252
*Management Anti-Fraud Programs
 and Controls*, 68
 Management override, 28
 Management's Discussion and
 Analysis (MD&A), 97–98
 Material amounts, 4
 Materiality, 13, 84

Material weaknesses, 4, 84,
 241–243

Matrixes, 141–147

benefits of using, 142

drawbacks of using, 142

example, 143–147

tips for preparing, 142–143

MD&A, *see* Management's Discussion
 and Analysis

Measurement (financial statement
 assertion), 213

Misstatement risk, 5–6

assessment of, 8, 13–14

and evaluation of control

deficiencies, 240–241

and fraud risk, 12–13

identification of, 8–13

identification of control for

mitigation of, 8

and managing change, 10–11

and materiality, 13

qualitative aspects of, 13–14

sources of, 9–10

Monitoring:

control objectives for, 79, 165

in COSO framework, 28, 30

and documentation, 115–116

of entity-level controls, 183–185

of financial information, 67

of other controls, 66–67

and project scoping, 65–67

and small business, 47

Motivations, for fraud, 13

Multiple locations, company with,
 85–86

N

Narratives, 137–141

benefits of using, 137

drawbacks of using, 137

tips for preparing, 138–141

National Commission on Fraudulent
 Financial Reporting, 26

- Networks, 180
 Norms, and corporate culture, 55
- O**
- Objectivity, 21
 of auditors, 22
 and COSO framework, 35, 37
 Observation, 181–183, 231
 Occupational Safety and Health Administration (OSHA), 63
 Occurrence (financial statement assertion), 213
 OECD (Organization for Economic Co-operation and Development), 166*n*.1
 Operating deficiencies, 239
 Operating effectiveness, of controls, 7
 Operating environment, changes in, 10
 Operating systems, 180
 Organizational structure:
 and control environment, 33–34
 and personnel policies, 57, 58
 Organization for Economic Co-operation and Development (OECD), 166*n*.1
 OSHA (Occupational Safety and Health Administration), 63
 Override, management, 28
 Overstatements, 241
- P**
- PCAOB, *see* Public Company Accounting Oversight Board
 PCAOB Auditing Standard No. 5, 21
 Period-end processes, 69–74
 characterization of, 70–71
 control objectives for, 78–79, 163–165
 importance of evaluating, 71
 routine vs., 70
 and selection/application of accounting principles, 71–74
 Personnel, new, 10
 Personnel handbook, 121–122
 Personnel policies:
 control objectives for, 77, 161–162
 in employee survey, 198
 and project scoping, 57–60
 Philosophy, management's, 33
 Physical controls, 40
 Pilot testing (with employee surveys), 174
 Planning, project, *see* Project planning
 Polo Ralph Lauren Corporation, 96–97
 Presentation (financial statement assertion), 213
 Preventive controls, and flowcharting, 130
 Private Securities Litigation Reform Act of 1995, 95
 Process, internal control as, 28
 Products, new, 11
 Project planning, 81–106. *See also*
 Scope of project
 action plan for, 107–109
 and business process activities, 82–83
 and company locations, 85–86
 and coordination with independent auditors, 103–105
 and determination of internal control deficiencies, 83–85
 and disclosure committee, 90–91
 documentation of, 105–106
 and gathering of information, 82–93
 and identification of focus areas, 83
 and internal audit activities, 89–90
 objective of, 81–82
 and sources of information, 93–99
 and structuring of project team, 100–103
 summary of planning questions, 110–113
 and use of third-party service organizations, 87–89
 “Prudent official” test, 243–245
 Public Company Accounting Oversight Board (PCAOB), 21, 241–242

Q

Quarterly reporting requirements, and evaluation of control deficiencies, 245–249

R

Rapid expansion, periods of, 11

Rationalizations, for fraud, 13

Real estate investment trusts (REITs), 131

Reasonable assurance, principle of, 29

“Reasonable basis,” 3–4

“Reasonable possibility,” 4

Reconciliations, 231

Redundant controls, 17

Reimbursement, of employees, for cell phone usage, 6

Reporting:

of deficiencies, 44

and evaluation of control

deficiencies, 245–249, 254–256

and IT general controls, 61–62

and project scoping, 69–74

Resources, providing necessary, 58

Responsibility(-ies):

assignment of, 34

and control deficiencies, 249–252

understanding/awareness of, 58

Restructurings, corporate, 11

Reviews, top-level, 39–40

Rights and obligations (financial statement assertion), 213

Risk, importance of understanding, 6–7

Risk analysis, and IT general controls, 179, 181

Risk assessment:

in COSO framework, 27, 30,

36, 38

and COSO Report, 35–38

and project scoping, 64–65

and small business, 46

Risk-based approach, 54–55, 214–217

Risk-based judgments, 4–7

Risk identification:

control objectives for, 78, 162–163

in COSO framework, 37–38

and project scoping, 62–65

Risk management, in COSO framework, 38

Risk of control failure, 5

Routine information, 42

Routine processes, 70

S

Sample size, 220–222

Sangamo BioSciences, Inc., 95–96

Sarbanes-Oxley Act of 2002 (SOX):

and changes to financial reporting, 1

and small business, 45, 47

Sarbanes-Oxley automated compliance

tools, 147–155

documentation process with, 150–151

functions of, 147–149

installation of, 149

and maintenance of information integrity, 151–152

and monitoring of documentation changes, 152

review features, 151

warehouse function of, 149–150

Scalability, of documentation

architecture, 126

Scope of project, 52–74. *See also*

Project planning

and anti-fraud programs/controls, 67–69

and corporate culture, 55–57

and information technology general controls, 60–62

and monitoring, 65–67

and period-end reporting, 69–74

and personnel policies, 57–60

and risk identification, 62–65

- and top-down approach, 54–55
 - Securities and Exchange Commission (SEC). *See* also Form 10K
 - and assessment of risk, 4–5
 - on control deficiencies, 241, 245, 246
 - and COSO report, 2
 - and disclosure committee, 90
 - on evaluation of internal control, 3–4
 - on internal control over financial reporting, 1–2
 - and items with higher risk of misstatement, 14
 - on management’s on-going direct involvement, in smaller companies, 184
 - MD&A rules of, 97–98
 - and monitoring controls, 66–67
 - on objective of management’s evaluation, 53
 - and objectivity vs. independence of parties involved, 21
 - Release Nos. 33-810 and 34-55928 of, 3
 - Rule 13a-15(f) of-2, 1
 - and top-down/risk-based approach, 55
 - Segregation of duties, 49
 - Senior management, role of, 42
 - Service organizations, 87–89
 - Shared activities, 220
 - Shared beliefs, 55–56
 - “Significant deficiencies,” 84, 244
 - Small business, applicability of COSO Report to, 44–48
 - SOX, *see* Sarbanes-Oxley Act of 2002
 - Statement of Accounting Standards No. 70, 245
 - Statement on Auditing Standards No. 55, 11
 - Statement on Auditing Standards No. 69, 37
 - Statement on Auditing Standards No. 70, 88, 89
 - Statement on Auditing Standards No. 99, 68
 - Subsidiaries, 53–54
 - Surveys, employee, 171–176, 194–200
 - data analysis, 175
 - evaluation of results, 196–200
 - example letter to employees, 194–195
 - example survey, 195–196
 - pilot testing with, 174
 - reporting of results, 175
 - selection of employees, 172–173
 - timing issues with, 173–174
 - writing questions for, 175–176
- T**
- Team, project, 100–103
 - Technology, incorporating new, 11
 - Temptations, 32
 - Testing techniques, for entity-level controls, 170–185
 - Tests, of activity-level controls, 214–233
 - and coordination with independent auditors, 232–233
 - design considerations with, 214, 234
 - documentation of, 232
 - evaluating results of, 217–220, 231–232
 - risk-based approach to, 214–217
 - sample sizes and extent of, 220–223
 - types of tests, 223–231
 - Timing factors, 43, 173–174, 215
 - Top-down evaluation approach, 8–23
 - and assessment of misstatement risk, 13–14

Top-down evaluation approach

(contd.)

and documentation, 115–116

and fraud risk, 12–13

and identification of misstatement
risk, 8–13and identification of relevant
controls, 15–20and identification of risk,
11–12and likelihood of control failure,
14–15

and managing change, 10–11

and project scoping, 54–55

and sources of risk, 9–10

and use of auditor, 20–23

Top-level reviews, 39–40

Training, 68

Transactions, events vs., in flowcharts,
129–130

U

Understatements, 241

V

Valuation (financial statement
assertion), 213

Values, and corporate culture, 55

Value system, and culture of
honesty/ethics, 68

Variable interest entities (VIEs), 91–92

VIEs, *see* Variable interest entities

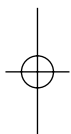
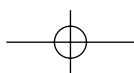
W

Walk-throughs, 209–211

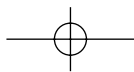
evaluating results of, 211

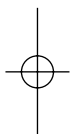
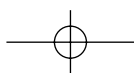
planning, 210

Weaknesses, material, 4

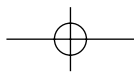


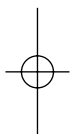
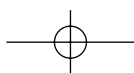
<http://www.pbookshop.com>



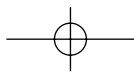


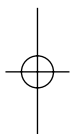
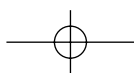
<http://www.pbookshop.com>



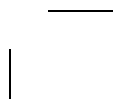
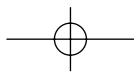


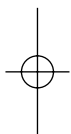
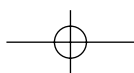
<http://www.pbookshop.com>



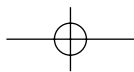


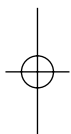
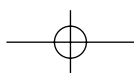
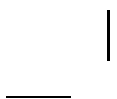
<http://www.pbookshop.com>



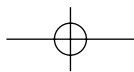


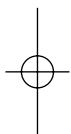
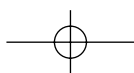
<http://www.pbookshop.com>



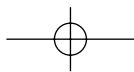


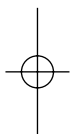
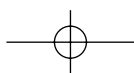
<http://www.pbookshop.com>





<http://www.pbookshop.com>





<http://www.pbookshop.com>

