

Index

A

- ACFE. *See* Association of Certified Fraud Examiners
- Affordable Care Act, 55, 67
- AICPA. *See* American Institute of Certified Public Accountants
- American Institute of Certified Public Accountants (AICPA). *See also* “CPA’s Handbook of Fraud and Commercial Crime Prevention”; SAS No. 99, *Auditor’s Consideration of Fraud in an Audit of Financial Statements* about, 2, 6, 12, 74
- AA-Guide, *Assessing and Responding to Audit Risk in a Financial Statement Audit*, 282
- “Achilles’ Heel of Fraud Prevention,” 225
- assertions, thirteen, 47
- Assessing and Responding to Audit Risk in a Financial Statement Audit*, 192
- Attestation Standards, 12, 275
- AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*, 238
- AU-C Section 265, 257, 297
- AU-C Section 315: *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, 126
- AU-C Section 317, 310
- AU-C Section 324 for public companies, 33
- AU-C Section 402, 34
- AU-C Section 402 *Service Organizations*, 33
- AU-C Section 530, *Audit Sampling, Audit and Accounting Guide* (AAG), 34, 179, 192, 258
- Audit and Accounting Guide on Sampling* (AAG-S), 199–200, 258
- Audit Guide: Assessing and Responding to Audit Risk in a Financial Statement Audit*, 337–38
- Auditing Standards, 103, 181, 198, 250
- ethics rule, 123
- A Framework for Evaluating Control Exceptions and Deficiencies*, 263
- Government Auditing Standards and Circular A-133 Audits Guide*, 203
- Management Antifraud Programs and Controls* (2002), 66
- Management Override of Internal Controls: The Achilles’ Heel of Fraud Detection* (2005), 66
- AT No. 50, *Attestation Standard*, 266
- AT No. 101, *Attest Engagements*, 303
- AT No. 501: *reports on internal controls*, 33, 316
- nonpublic companies, guidance to auditors of, 2
- Risk Assessment Standards, 318
- SAS No. 70, 154
- Section 101–3, *professional ethics*, 272
- Standards for Attestation Engagements No. 16, 123
- annual 10-K report, 314

- antifraud. *See also* fraud
 controls for management, 66–67
 processes and controls, evaluating, 80–82
 program, 72–73, 86 (*See also* SAS No. 99, *Auditor's Consideration of Fraud in an Audit of Financial Statements*)
 programs and controls, 64–66, 72–73, 86, 271, 273
- Association of Certified Fraud Examiners (ACFE), 63
- audit committee
 control activities, 159–60, 164
 control environment, 104–7, 118
 risk assessment, 44, 70, 80n5, 81–86
 SAS No. 99, *Auditor's Consideration of Fraud in an Audit of Financial Statements*, 82–84
- B**
- backup and recovery plans, 207
- Bank of America, 27
- Barings Bank, 26–27
- Bedard-Graham study, 281
- Berra, Yogi, 23, 250
- Beswick, Paul (SEC), 305
- board of directors
 control activities, 158–60, 163–64
 control environment, 104–5, 110, 117–18
 documentation project, 44
 risk assessment, 70, 74–75, 80–86
 SAS No. 99, *Auditor's Consideration of Fraud in an Audit of Financial Statements*, 82–84
- business risk, 102, 113
- C**
- California Civil Code Sections 1798.82 and 1798.29, 95
- CEO. *See* chief executive officer
- certified fraud examiner (CFE), 67
- certified public accounting (CPA), 217, 262, 319
- chief accounting officer, 84
- chief executive officer (CEO), 75, 82, 217, 240, 319
- chief financial officer, 84, 228, 265, 319
- chief information officer, 332
- chief operating office, 74
- ChoicePoint, 96
- COBIT. *See* Control Objectives for Information and related Technology
- code of conduct, 73, 75–80, 83, 85, 87, 103, 119
- code of ethics, 78
- Code of Ethics Statement (of FEI), 91–92
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). *See also* Principles of 2013 COS Framework
 1992 Framework Guidance, 6
 2006 Framework Guidance, 20
 Principles of, 6, 9–10
 2013 Framework, 17 Principles in, 5
 2013 Framework, transitioning to COSO, 9–10
 2013 Framework Guidance, 7–8, 10–11
 approach, flexible, adaptable, no one-size-fits-all, 16–17
 approach, objective-driven, 16
A Compendium of Approaches and Examples, 158
 controls vs. processes, 14–18
 COSO Framework (1992; 2013), five interrelated components of the, 3–5
 cost–benefit requirements, debate of, 18
 internal control has limitations, 15–16
 internal control integrated framework overview, 2

- Internal Control—Integrated Framework: Evaluation Tools* (1992), 2, 158, 338
- Internal Controls Framework* (2013), revised COSO, 6–8
- Internal Controls over Financial Reporting—Guidance for Smaller Public Companies* (2006), 146, 329
- maintenance, basic scoping and strategies for, 11–12
- people factor, 17–18
- private companies, 14
- reasonable assurance, 17
- Section 302 certificates, 319
- Section 404 certificates, 319
- Smaller Public Company*, 185
- SOC No. 1, 7, 136
- SOC No. 2, 7, 176
- triangle of efficiency, 13–14
- what we must do, 8–11
- where we depart, 12–13
- compensating controls, 260–61, 269, 287–90, 294–97, 301
- compensation programs, 112
- competence, 103, 110–12, 114, 116, 118
- complementary controls, 296
- compliance and entity values (CE), 66
- control activities
 - 1992 Framework, 128, 130, 132
 - 2013 Framework, 128–29, 132, 143–45
- accounts vs. transaction cycles, 129
- assertions, role of, 124–27
- assertions vs. control objectives, 127–29
- audit committee, 159–60, 164
- automated controls, 130–32, 135, 162
- board of directors, 158–60, 163–64
- change controls, 137–38
- COBIT and the IT Governance Institute, 140–41
- commitments and contingencies, 152–53
- controls, examples of, 145
- dependency, determining, 132–34
- detective controls, 130, 162
- equity, 153–54
- fixed assets, 150–51
- generic cycle, 157
- goodwill and intangibles, 151
- inventory, 148–49
- investments, 154
- IT environment, 131, 135, 139, 141
- IT-related controls, 134–40
- loans (financial institutions), 156–57
- mix of controls types and levels of application, 130–31
- new framework, transitioning to, 144–45
- new systems development, 138–39
- operations and maintenance, 139–40
- payroll and benefits, 149–50
- period end (quarterly and/or annual) process, 156
- preventive controls, 124, 130
- Principle 1: demonstrates commitment to integrity and ethical values, 158
- Principle 2: exercises oversight responsibility, 159
- Principle 3: establishes structure, authority, and responsibility, 142, 159
- Principle 4: demonstrates commitment to competence, 143, 159
- Principle 5: enforces accountability, 158, 160
- Principle 6: specifies clear objectives, 160
- Principle 7: identifies and analyzes risk, 160
- Principle 8: assesses fraud risk, 160–61
- Principle 9: identifies and analyzes significant changes, 161

- control activities (*Continued*)
 - Principle 10: selects and develops
 - control activities to mitigate risks, 120–32, 145, 159–62, 164
 - Principle 11: selects and develops information technology general controls, 120, 131–34, 142, 145, 162
 - Principle 12: deploys controls through policies and procedures, 120, 141–43, 145, 158–61, 163
 - Principle 13: uses relevant information, 120, 133, 163
 - Principle 14: communicates internally, 133, 163
 - Principle 15: communicates externally, 158, 163–64
 - Principle 16: conducts ongoing and/or separate evaluations, 164
 - Principle 17: evaluates and communicates deficiencies, 164
- purchasing and cash disbursements, 148–49
- revenue, 147
- risk assessment, 121–24
- security and access, 136–37
- segregation of duties, 131–32
- summing up, 143–44
- tax accrual and compliance, 151–52
- treasury, 154–56
- control criteria, 1–2
- control deficiencies
 - accounting expertise, in-house, 272
 - adjusted exposure, 287, 289, 296, 300
 - application controls, 258–59, 274, 280, 290–91, 293, 296–97
 - assessment, overall, 281–82
 - automated control, 249, 261, 265, 277–78, 280, 296
 - business characteristics and risk environment, 268–70
 - compensating controls, 260–62
 - control, purpose and level of, 264–65
 - control deficiencies, automated, 277–78
 - control deficiencies, conditions indicating, 270–76
 - control deficiencies, evaluating process/transaction-level, 269
 - control deficiencies, internal, 249n1, 253, 265n9
 - control deficiencies, IT general, 279–80
 - control deficiencies, manual, 277
 - control deficiencies and definitions, 252–63
 - control deficiencies in pervasive controls other than ITGC, evaluating, 293–96
 - control deficiency, 251, 255, 260–62, 267–68, 272, 277–78, 285–87, 291–92, 294, 296, 300
 - control environment, 256, 260, 265, 271, 273–74, 281
 - control objective, 248, 252, 260, 269, 277–78, 280, 287–89, 291–92, 296–98
 - controls performance, inadequate evidence of, 275–76
 - deficiencies, aggregating, 280–81
 - deficiencies, examples of more severe, 271
 - deficiencies, framework for assessing severity of, 262–63
 - deficiencies, inevitable, 248–51
 - deficiencies, other, 272–73
 - deficiencies and exceptions, 259–60
 - deficiencies that may be material weaknesses, special, 256–58
 - deficiency, design, 252, 255, 274, 278
 - deficiency, key factors to assess severity of, 263–70
 - deficiency, operating, 252, 274, 290
 - documentation, inadequate, 273–75
 - exceptions found in operating effectiveness, evaluating, 285–87

- exceptions found when testing
 - operating effectiveness, 268
- gross exposure, 267, 287, 289, 296–97, 300
- guiding principles, 285–96
- IT general controls (ITCGs), 258–59, 266–67, 270, 273, 277–81
- ITGC deficiencies, evaluating, 290–93
- material misstatement, 253–56, 258, 269, 271, 277, 288–89, 294, 297
- material weakness, 248, 250, 252–67, 269–72, 276, 278–81, 284, 286, 288–92, 294–97, 299
- material weakness deficiencies over time, 276
- misstatement, assessing the likelihood and significance of possible, 254–56
- not-for-profit company, 250, 270, 275
- objectives and timing, 265–67
- pervasive controls other than ITGC, 285, 293–97
- potential misstatement, 255, 277, 286, 297–98
- Principle 11: selects and develops information technology general controls, 259
- private companies, 250–51, 263, 270
- process/transaction-level control deficiencies, 287–90
- “prudent official” test, 262
- public and private company standards alignment for assessing deficiency severity, 251–52
- public companies, 248–49, 251–53, 260, 263, 266, 270, 273, 276
- purpose, 283–85
- redundant controls, 269, 287–89, 291, 298
- terminology, 296–98
- upper limit deviation rate, 286, 296–98
- upper limit in percent, calculate, 300
- upper limit related to the magnitude of exposure, 300–301
- weaknesses over time, 276
- when is material weakness not a material weakness?, 258–59
- control environment
 - 2013 Principles, transition to, 115–16
 - audit committee, 104–7, 118
 - board of directors, 104–5, 110, 117–18
 - governance and, 104–8, 113, 117
 - management’s philosophy and operating style, 102
 - Principle 1: demonstrates commitment to integrity and ethical values, 100–103, 108, 110, 114, 116
 - Principle 2: exercises oversight responsibility, 104–8
 - Principle 3: establishes structure, authority, and responsibility, 109–10
 - Principle 4: demonstrates commitment to competence, 103, 110–13, 116
 - Principle 5: enforces accountability, 113–16
 - Principle 8: assesses fraud risk, 113, 115, 118
 - Principle 10: selects and develops control activities to mitigate risks, 110
 - Principle 14: communicates internally, 115
 - Principle 16: conducts ongoing and/or separate evaluation, 110
 - Principle 17: evaluates and communicates deficiencies, 110, 114
- Control Objectives for Information and related Technology (COBIT), 140–41, 204
- control responsibilities
 - audit committee, 118
 - board of directors, 118
 - chief executive, 117

- control responsibilities (*Continued*)
- finance officers, 118
 - internal auditors, 119
 - management, 118
 - personnel, other, 19
- corruption, 62–64, 76, 76n1, 81, 85
- Corruptions Transparency Index, 64
- COSO. *See* Committee of Sponsoring Organizations of the Treadway Commission
- “CPA’s Handbook of Fraud and Commercial Crime Prevention,” 87–90. *See also* fraud
- clients and suppliers relationships, 88
 - code of conduct, organizational, 87
 - communications, prompt, 90
 - conflicts of interest, 88
 - employee conduct, 87–88
 - gifts, entertainment, and favors, 88
 - kickbacks and secret commissions, 88–89
 - organization funds and other assets, 89
 - organization records and communications, 89
 - outside activities, employment, and directorships, 88
 - outside people and organizations, dealing with, 29
 - privacy and confidentiality, 90
- credit cards, business, 101
- customer complaints, 174
- cycle counts of inventory, 226
- D**
- dashboard, 175
 - data element mapping, 207
 - data-mining thieves, 55
 - disaster and recovery plan, 140
 - disaster recovery, 208–10
 - documentation project. *See also* scoping inquiries summary
 - be careful out there!, 40–41
 - business objectives, 21–24
 - disclosure committee (public companies only), 40
 - financial statements, mapping the entity to the, 25–26
 - fraud, 22–23, 27, 38, 44
 - “in scope” does it imply extensive testing?, 37–39
 - initial year, after the, 24–25
 - internal audit activities, 34–35
 - investment and merger scoping considerations, 35–37
 - locations, multiple, 29–31
 - overstatement and understatement, 28–29
 - risk, inherent and control, 28
 - risks as not just quantitative measures, 27–28
 - scope set by financial statements, 26
 - scope set by revenue, 22
 - service organizations and outsourcing, 31–34
 - Dodd-Frank Act of 2010, 13, 18, 67, 319
 - dual signatures, 49
- E**
- EITF. *See* Emerging Issues Task Force
 - Emerging Issues Task Force (EITF)
 - Consensus Position* 00–1, 36
 - employee survey. *See* sample practice aids
 - Enron, 23, 165, 250
 - Environmental Protection Agency (EPA), 50
 - Ernst & Young survey, 249
 - ethical
 - behavior, 74, 76, 78–79, 83, 92
 - values, 273
 - ethics officer, 78
 - ethics policy, 103
 - European Spreadsheet Risks Interest Group, 133
 - evidence and testing. *See also* sample practice aids; sample size tutorial
 - auditor alert, 197
 - auditor caution, 183

- corroborating information, 191
 - corroborative inquiry, 188
 - documentation, 184–85
 - efficiency tip, 181
 - evidence, 184
 - evidence, sufficient, 179–87
 - evidence, types of, 187–88
 - external auditors, 215
 - financial statement areas, 197
 - functioning, 188–89
 - independent auditors, 182–83, 185–87
 - information, gathering, 187–93
 - inquiries, suggestions for, 190–91
 - internal auditor, 180, 182, 185, 199, 204, 215
 - internal controls, 180–83, 186–87, 189, 191, 195, 197, 203–4, 210
 - IT general controls (ITCGs), 204–5, 209–10
 - nonsampling situations, 202–3
 - objective, your, 181–83
 - operating controls, infrequently, 201
 - plans, best-laid, 209
 - Principle 11: selects and develops
 - information technology general controls, 194, 204
 - reporting date issues for internal controls opinions, 195–97
 - sad story, 191–92
 - sample size guidance, 203–4
 - sample size tutorial, 211–16
 - sample sizes for computerized controls, 202
 - sampling and sample sizes, 198–202
 - test of one, 189
 - test timing, 195
 - testing and sampling, 194–202
 - testing new system development and implementation, 207–8
 - testing operations, 208–9
 - testing program modifications, 206–7
 - testing security and access controls, 205–10
 - tests, factors determining the extent of, 201
 - top-down concept, 194–95
 - true story, 208
 - walk-through, 181, 186, 188–95
 - Exchange Act filings, 40
 - external auditors, 168, 174, 215
- F**
- fair value determination, 183
 - FASB. *See* Financial Accounting Standards Board
 - FDA. *See* Food and Drug Administration (FDA)
 - Federal Communications Commission (FCC), 50
 - Financial Accounting Standards Board (FASB)
 - Concept Statements, 53
 - Interpretation Number (FIN) 46, 36
 - Statement No. 5: *Accounting for Contingencies*, 253–54
 - Financial Executives International (FEI)
 - Code of Ethics Statement, 91–92
 - focus groups, 227–28
 - Food and Drug Administration (FDA), 50
 - Foreign Corrupt Practices Act in 2012, 62, 64
 - forms and templates
 - 1992 COSO *Internal Control—Integrated Framework: Evaluation Tools*, 338
 - 2006 COSO *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*, 329
 - 2013 Framework examples, 340–47
 - component and final assessment, 346–47
 - control environment component
 - evaluation summary, 372
 - deficiency summary, 346
 - documentation of financial reporting
 - software and spreadsheets, 364–67

- forms and templates (*Continued*)
- form, sampling, 345–46
 - form, walk-through, 342–44
 - forms, principle-based
 - information-gathering, 341
 - forms, transaction-based, 342
 - forms and reports, some illustrative, 341–47
 - historical perspective, 338–40
 - information technology general controls assessment form, 355–63
 - information-gathering form—
 - principle focused, 348–49
 - information-gathering form—revenue, 350–52
 - internal control deficiencies summary, 371
 - IT general controls (ITCGs), 344
 - Principle 1: demonstrates commitment to integrity and ethical values, 371–72
 - Principle 10: selects and develops control activities to mitigate risks, 341
 - Principle 11: selects and develops information technology general controls, 340
 - Principle 12: deploys controls through policies and procedures, 341–42
 - sampling form for tests of controls, 368–70
 - software and spreadsheets and standing data files, 344–45
 - story, true, 343
 - walk-through documentation form, 353–54
 - work papers, flow of, 340
- for-profit business organization, 106
- The Fortune Cookie*, 175
- fraud. *See also* antifraud; “CPA’s Handbook of Fraud and Commercial Crime Prevention”; SAS No. 99, *Auditor’s Consideration of Fraud in an Audit of Financial Statements*
- Principle 8: assesses fraud risk, 5, 20, 62–65, 113, 115, 118, 160–61, 236–37
 - “Achilles’ Heel of Fraud Prevention,” 225
 - AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*, 238
 - auditor responsibility to detect fraud, 65
 - Guidance To Help Prevent, Deter, and Detect Fraud*, 72
 - Management Antifraud Programs and Controls* (2002), 66
 - Management Override of Internal Controls: The Achilles’ Heel of Fraud Detection* (2005), 66
 - National Commission on Fraudulent Financial Reporting, 2
- fraud officer, 78
- fraud prevention, 65–66, 75, 86
- fraud risk assessment
- about, 62, 65, 80–81, 86
 - equipment, inventory, and anything not bolted down, 95
 - fraud, detecting, 97–98
 - fraud risk areas and schemes, common, 93–96
 - fraud triangle, 96–97
 - inventory mischief, 96
 - payroll, 95
 - personal information risks, 95–96
 - purchasing and cash disbursements, 94–95
 - sales and cash receipts, 94
- fraud risk-management program, 81
- Funk, Arlene, 221, 221n1
- G**
- gambling habit, 103
 - GAO. *See* Government Accountability Office

- generally accepted accounting principles (GAAP), 9, 168, 181, 184, 251, 267
- governance
 control environment and, 104–8, 113, 117
 information and communication and, 167–71
 reporting requirements, 303, 314, 317
- Government Accountability Office (GAO)
 about, 272, 303, 330
 Account Risk Analysis (ARA) forms, 129
Financial Auditing Manual, 129
 Specific Control Evaluation (SCE) forms, 129
- Great Salad Oil Swindle, 96
- H**
- harassment policy, 273
How to Conduct Surveys (Funk), 221
 human resources (HR), 103, 111, 226
 Hurricane Katrina, 50, 140
 Hurricane Sandy, 50, 140
- I**
- IIA. *See* Institute of Internal Auditors
- incentives, 101, 112–13
- independent auditors, 175, 182–83, 185–86
- information and communication
 external communications, 170
 informal communications, 168
 information, importance of, 167
 new framework, transitioning to, 171–72
- Principle 10: selects and develops control activities to mitigate risks, 166
- Principle 12: deploys controls through policies and procedures, 166, 169
- Principle 13: uses relevant information, 166–68, 172
- Principle 14: communicates internally, 168–70
- Principle 15: communicates externally, 170–72
- Information Systems Audit and Control Association (ISACA), 140
IT Control Objectives for Sarbanes-Oxley, 323
- information technology (IT), 54–55, 81
 auditors, 189
 professionals, 131, 139–41
 specialist, 114
- Information Technology Control Objectives for Sarbanes-Oxley*, 205, 323
- information technology general controls (ITGCs)
 about, 54–55, 258
 control deficiencies, 258–59, 266–67, 270, 273, 277–81
 evidence and testing, 204–5, 209–10
 forms and templates, 344
 reporting requirements, 308–9
- Information Technology Governance Institute (ITGI)
IT Control Objectives for Sarbanes-Oxley, 323
- Institute of Internal Auditors (IIA), 34–35, 233
Standards for the Professional Practice of Internal Auditing (IIA Standards), 85
- Institute of Management Accountant's Ethics Center, 77
- intellectual property rights, 167
- internal auditors
 about, 34–35
 control environment, 107, 110, 119
 documentation project, 34–35
 evidence and testing, 180, 182, 185, 199, 204, 215
 monitoring, 175
 reports, 171
 risk assessment, 65, 80, 83, 85–86

- internal control(s)
 auditing standard, 105
 deficiencies, 177–78
 evidence and testing, 180–83,
 186–87, 189, 191, 195, 197,
 203–4, 210
 over financial reporting, 252, 302,
 304–5
 performance, 173
 project management and tools
 assessment design, 319–24,
 328–29, 332–35
- Internal Revenue Service
 Form 990, 275
 Form 990 A, 275
- interviews. *See* questionnaire
 development and interviews
- Iran
 Advisory on the Use of Exchange
 Houses and Trading Companies to
 Evade U.S. Economic Sanctions
 Against Iran, 62
 Amendment of Iranian Financial
 Sanctions Regulations to
 Implement Sections 503 and 504
 of Threat Reduction Act and
 Provisions of Executive Order
 13622, 62
 Guidance re Iran Threat Reduction
 and Syria Human Rights Act of
 2012, 62
 Iran Freedom and Counter-
 Proliferation Act of 2012,
 62
 Iran Sanctions Loophole Elimination
 Act of 2013, 61
 Nuclear Iran Prevention Act of 2013,
 61
- ISACA. *See* Information Systems
 Audit and Control
 Association
- ISO/IEC 27001, 137
 ISO/IEC 27002, 137
 IT. *See* information technology
- IT Governance Institute (ITGI)
IT Control Objectives for Sarbanes Oxley,
 141
- ITGCs. *See* information technology (IT)
 general controls
- J**
- JOBS Act of 2012, 18
- L**
- legal counsel, 177
 Lie, Dr. Eric, 24
 litigation exposure, 184
- M**
- management discussion and analysis
 (MD&A), 309
 management intervention, 102
 material weaknesses
 about, 136, 160, 164
 deficiencies over time, 276
 identified controls deficiencies,
 assessing severity of, 248, 250,
 252–67, 269–72, 276, 278–81,
 284, 286, 288–92, 294–97, 299
 management's year-end report, 306
 in risk assessment, 62
 significant deficiency and, 44
 special deficiencies, 256–58
 when is a material weakness not a
 material weakness?, 258–59
- Matthau, Walter, 27
- MD&A. *See* management discussion and
 analysis
- mission statement, 103
- monitoring
 oversight procedures, 173, 175
 Principle 3: establishes structure,
 authority, and responsibility, 176
 Principle 4: demonstrates commitment
 to competence, 174
 Principle 5: enforces accountability,
 176

- Principle 7: identifies and analyzes risk, 174
- Principle 9: identifies and analyzes significant changes, 174
- Principle 10: selects and develops control activities to mitigate risks, 176
- Principle 14: communicates internally, 176
- Principle 16: conducts ongoing and/or separate evaluations, 174–76
- Principle 17: evaluates and communicates deficiencies, 176–78
- revised framework, transitioning to, 177–78
- N**
- National Association of Securities Dealers (NASD), 106
- National Commission on Fraudulent Financial Reporting, 2
- New York State Information Security Breach and Notification Act, 95–96
- New York Stock Exchange, 106
- nonaccelerated filers, 182–83
- Nonprofit Integrity Act of 2004, 275
- nonpublic companies, 195
- nonstatistical sampling methods, 219
- North Korea Nonproliferation and Accountability Act of 2013, 61
- not-for-profit company, 250, 270, 275
- not-for-profit foundations, 104
- O**
- Office of Management and Budget (OMB), 13, 47, 201, 203
- oral evidence, 188
- Orange County, CA, 27
- P**
- paper-tiger mentality, 113
- Parmalat, 23
- passwords, 203, 206
- PCAOB. *See* Public Company Accounting Oversight Board
- performance and rewards structure, 113
- performance targets, 101
- personal identifying information, 136
- POF. *See* point of focus
- point of focus (POF), 11
- PricewaterhouseCoopers whitepaper on spreadsheets, 133, 202
- Principles of 2013 COS Framework
- Principle 1: demonstrates commitment to integrity and ethical values, 20, 100–103, 108, 110, 114, 116, 158, 234–35, 371–72
- Principle 2: exercises oversight responsibility, 20, 104–8, 159
- Principle 3: establishes structure, authority, and responsibility, 20, 109–10, 142, 159, 176, 235
- Principle 4: demonstrates commitment to competence, 10, 20, 103, 110–13, 116, 143, 159, 174
- Principle 5: enforces accountability, 20, 113–16, 158, 160, 176
- Principle 6: specifies clear objectives, 20, 56–59, 160, 236
- Principle 7: identifies and analyzes risk, 20, 56–59, 160, 174, 236
- Principle 8: assesses fraud risk, 5, 20, 62–65, 113, 115, 118, 160–61, 236–37
- Principle 9: identifies and analyzes significant changes, 17, 20, 26, 66–67, 161, 174
- Principle 10: selects and develops control activities to mitigate risks, 20, 59, 110, 120–32, 145, 159–62, 164, 166, 176, 341
- Principle 11: selects and develops information technology general controls, 5, 20, 54, 120, 131–34, 142, 145, 162, 194, 204, 259, 340

Principles of 2013 COS Framework

(Continued)

- Principle 12: deploys controls through policies and procedures, 20, 120, 141–43, 145, 158–61, 163, 166, 169, 237, 341–42
 - Principle 13: uses relevant information, 20, 61, 120, 133, 163, 166–68, 172
 - Principle 14: communicates internally, 20, 61, 115, 133, 163, 168–70, 176
 - Principle 15: communicates externally, 20, 61, 158, 163–64, 170–72
 - Principle 16: conducts ongoing and/or separate evaluations, 20, 110, 164, 174–76, 237–38
 - Principle 17: evaluates and communicates deficiencies, 20, 110, 114, 164, 176–78, 237–38
 - 2013 COSO guidance and, 7–11
 - Type 2 Service Organizations* report, 305
 - privacy laws, 55
 - private companies
 - control deficiencies, 250–51, 263, 270
 - COSO, 14
 - project management and tools
 - assessment design, 318
 - private enterprises, 104
 - project management and tools
 - assessment design
 - archiving capability, 330–31
 - backups and recovery, 329
 - contextual help screens, 328
 - criteria, additional, 329–31
 - cross referencing and linking, 328
 - flexibility and adaptability, 327
 - forms migration, 329–30
 - independent auditors, 334–36
 - internal control, 319–24, 328–29, 332–35
 - network compatible, 327
 - one-write capability, 328
 - operations and accounting personnel, 321–22
 - pilot project, value of a, 331–34
 - project management, 318–19
 - project team, structuring, 319–26
 - project team members, 320–21
 - responsibilities and lines of reporting, 319–20
 - status indicators and warnings, 328–29
 - technical specialists, 322–24
 - testing and evaluation teams, 324
 - tool solution features, 326–31
 - tools assessment design, 325–26
 - user interface design, 327
 - work paper discipline, 329
 - public companies
 - control deficiencies, 248–49, 251–53, 260, 263, 266, 270, 273, 276
 - evidence and testing, 182, 185–86, 195–96, 230, 235
 - project management and tools
 - assessment design, 318–19, 323, 325, 330, 335–36
 - Public Company Accounting Oversight Board (PCAOB), 6, 11, 14, 179
 - Auditing Standard AS No. 2:, 21, 31, 194, 250
 - Auditing Standard AS No. 4, 314–15
 - Auditing Standard AS No. 5, 21, 31, 38–39, 54, 182, 186, 253, 297, 303, 310–11, 313–14, 320, 322
 - Auditing Standard AS No. 15, 126–27
 - auditing standards, 103
 - cost control, 46
 - Statement on Standards for Attestation Engagements (SSAE) No. 15, 303
 - public disclosures, 197
- Q**
- quarterly 10-Q reports, 314
 - questionnaire development and interviews. *See also* sample practice aids

controls, reporting on, 230–31
 data analysis and reporting results,
 222–23
 entity-level controls and management,
 232–34
 focus groups, 227–28
 inquiries for walk-throughs, 232–34
 interview follow-up, 231
 interview procedures, setting the scope
 of, 230–31
 interview process, 228–30
 interviews, conducting, 224–25
 interviews, examples of use, 225–26
 interviews, planning and strategy for,
 226–27
 interviews, tips for effective and
 efficient, 228
 management inquiries: sample
 questions, 234–38
 Principle 1: demonstrates commitment
 to integrity and ethical values,
 234–35
 Principle 3: establishes structure,
 authority, and responsibility, 235
 Principle 6: specifies clear objectives,
 236
 Principle 7: identifies and analyzes
 risk, 236
 Principle 8: assesses fraud risk, 236–37
 Principle 12: deploys controls through
 policies and procedures, 237
 Principle 16: conducts ongoing and/or
 separate evaluations, 237–38
 Principle 17: evaluates and
 communicates deficiencies,
 237–38
 survey, testing the, 221–24
 survey questions, writing, 223–24
 surveys, common problems, 219
 surveys, Web-based, 222, 240
 surveys of employees, 219–24
 when and how often?, 221
 whom and how many to survey?,
 219–21

R

random selection procedures, 219
 records of complaints, 170
 Red Cross, 303
 regulators, 168, 170
 regulatory agency, 171
 regulatory issues, 167
 Release of 2012 Terrorist Assets Report,
 62
 reporting requirements
 AICPA report on internal controls,
 illustrative, 316–17
 as-of reporting implications, 307–9
 auditor reports on internal control,
 independent, 311–12
 auditors and legal counsel,
 coordinating independent, 315
 communications, company and
 auditor, 312–14
 financial statements and internal
 controls, 312
 management's report on material
 weakness at year-end, 306
 management's responsibilities for
 internal control, 309–12
 nonpublic entity reporting, 302–3
 public company annual and quarterly
 reporting requirements, 304–5
 reporting the remediation of
 weaknesses, 314–15
 risk assessment
 2013 principles, transitioning to,
 70–71
 antifraud controls for management to
 consider, 66–67
 assertions, 51–55
 assessments of inherent and control
 risks, 50–51
 auditor responsibility to detect fraud,
 65
 balance sheet accounts at period-end,
 53
 basics, 47–48
 compliance objectives, 58

- risk assessment (*Continued*)
- compliance risks, 61–62
 - control environment, 45, 81, 84
 - cost control, 46–47
 - financial reporting objectives, external, 58
 - financial statements, presentation and disclosure in, 53–54
 - income statement and current-period transactions, 52–53
 - information gathering to support the risk assessment and consider change, 68–69
 - information technology issues and risk assessment, 54–55
 - inquiries and corroboration, 70
 - internal reporting objectives, 58
 - material weaknesses in, 62
 - nonfinancial reporting objectives, external, 58
 - operations objectives, 57–58
 - Principle 6: specifies clear objectives, 56–59
 - Principle 7: identifies and analyzes risk, 56–59
 - Principle 8: assess fraud risk, 62–65
 - Principle 9: identify and assess significant change, 66–67
 - Principle 10: select and develops control activities to mitigate risks, 59
 - Principle 11: selects and develops information technology general controls, 54
 - Principle 13: uses relevant information, 61
 - Principle 14: communicates internally, 61
 - Principle 15: communicates externally, 61
 - Risk Assessment Principles: 2013 vs. 2006, 70
 - risk assessment principles in COSO, 46
 - risk information, external sources of, 60–61
 - risk information, internal sources of, 61
 - risk measurement using likelihood and magnitude, 49
 - risks, identifying, 59–61
 - risks and changes, consideration of, 69
 - statistics, some, 63–65
 - ties to other principles and components, 66
 - upper management and, 65, 82
- Russian aggression in Crimea and the Ukraine, 62
- S**
- SALY. *See* same as last year
- same as last year (SALY), 24, 67
- sample practice aids. *See also* evidence and testing; questionnaire development and interviews
- employee survey, sample, 241–42
 - employee survey of corporate culture and personnel policies, sample, 240–42
 - employee survey results, guidance on the evaluation of, 242–45
 - letter to employees in advance of employee survey, sample, 239–40
 - walk-throughs and transaction controls sample, 245–47
- sample size tutorial. *See also* evidence and testing
- AU-C No. 530, Audit Sampling, 211
 - decision rule for results, 213
 - deviations, cautions about, 216
 - sample size formula, 212–13
 - sample sizes, computer-determined, 215–16
 - sample sizes determined using a table, 213–14
 - sampling plan, two-stage sequential, 215

- Sarbanes-Oxley (SOX) Act of 2002
 about, 5, 18, 24, 55, 123, 176, 179,
 250, 309, 318
 Section 302, 176, 235, 310
 Section 404, 62, 176, 194
- SAS No. 99, *Auditor's Consideration of Fraud in an Audit of Financial Statements*. *See also* American Institute of Certified Public Accountants;
 fraud
 about, 65–66, 72–76, 238
 antifraud processes and controls, evaluating, 80–82
 audit committee or board of directors, 82–84
 auditor's considerations, 72–73
 confirmation, 79–80
 culture of honesty and high ethics, creating, 76–86
 discipline, 80
 employees, hiring and promoting appropriate, 78–79
 fraud risks, identifying and measuring, 80–81
 fraud risks, mitigating, 81
 fraud triangle, 96–97
Guidance To Help Prevent, Deter, And Detect Fraud, 72–74
 independent auditors, 86
 information, other, 86
 internal auditors, 85
 internal controls, implementing and monitoring, 81–82
 management, 84
 oversight process, 82–86
 preface, 74
 tone at the top, setting the, 76–77
 training, 79
 workplace environment, creating a positive, 77–80
- scoping inquiries summary
 company operations and industry characteristics, 42–43
 deficiency and material weakness, existence of significant, 44
 engagement scope, 43
 internal control considerations, 43–44
- SEC. *See* Securities and Exchange Commission
SEC v. Livent, 279
- Securities and Exchange Commission (SEC)
 about, 1–2, 7, 13, 105, 123, 176, 179, 183, 318
 Blue Ribbon Commission on audit committees, 105–7
 cost control, 46
 internal control, 166
 public companies, 14
 Release No. 33–8238, 304
 Release No. 33–8809, 218
 Release No. 33–8810, 30–31, 252, 256, 260, 304–6, 312
 Release No. 34–47986, 304
 SEC 10-K annual filing, 13
 SEC Form 10-K, 36, 42–43
- Security Breach and Notification Act, 96
 security breaches, 49, 96
 segregation of duties, 167
 service organization controls (SOC), 34
 significant deficiency, 136
 social media, 171
 software testing, 208
 sole proprietorship, 108
 standards of conduct, 100
- Statement of Auditing Standards.
See also SAS No. 99, *Auditor's Consideration of Fraud in an Audit of Financial Statements*
Guidance To Help Prevent, Deter, and Detect Fraud, 72
- statistical sampling methods, 220
 stratified samples yield, 220
 surveys. *See* questionnaire development and interviews; sample practice aids

Syria

- Guidance re Iran Threat Reduction and Syria Human Rights Act of 2012, 62
- Syria Transition Support Act of 2013, 61
- systems development life cycle, 139

T

- Target Stores, 49
- tax shelter, aggressive, 101
- temptations, 101
- terrorist attacks of 9/11, 140
- thirty-fifth of December, 53
- training programs, 72, 78
- Treasury Department, 67
- Turnbull Report (United Kingdom), 2
- Type I reports, 34, 176
- Type II report, 33–34, 176

U

- United Way, 303
- upper limit methodology, 278
- upper management, 65, 82

V

- variable interest entities (VIEs), 36
- VIEs. *See* variable interest entities

W

- Wall Street Journal*, 171
- Web-based surveys, 222, 240
- whistleblower policies, 273
- WorldCom, 23, 250

Y

- Y2K, 137–39

Z

- ZZZBest, 27



<http://www.pbookshop.com>





<http://www.pbookshop.com>





<http://www.pbookshop.com>





<http://www.pbookshop.com>





<http://www.pbookshop.com>





<http://www.pbookshop.com>

