

Index

A

- acceptance testing, 290, 301
- accounting control model, 272
- accounting policies and procedures
 - accountancy policy control model, 271
 - accounting control model, 272
 - accounting environment, 257–59
 - accounting policy selection and application controls, 266–72
 - accounting principles, 263–65
 - accounting staff, incompetent, 262–63
 - adjusting entries, 245, 266, 270
 - analytical review, 268–69
 - applications, computational errors in, 265
 - application systems, reliance on, 265–66
 - assumptions, fallacious underlying, 265
 - attributes, overlooked essential, 264
 - audit, 269
 - audit committee, 249, 270
 - chief accounting officers, uninformed, 262
 - code of ethics, 266–67
 - consultation, outside, 267
 - counterparty treatment, 270
 - estimates, unreasonable underlying, 265
 - GAAP to IFRS conversion, 259–61
 - incomplete facts, 263
 - personnel selection, 267
 - quantitative estimation methods, 268
 - reference literature, 266–67
 - regulatory
 - examination/investigation, 269
 - restatement, 270–71
 - side agreements, incomplete, 263
 - substance, form over, 264
 - supervision and review, 268
 - training and education, 268
 - transactions, misclassified, 265
 - what can go wrong with, 262–66
 - whistleblowers, 269
 - written communication, 267–68
- accounting principles, 110, 263–65.
 - See also* generally accepted accounting principles (GAAP); *Statutory Accounting Principles* (SAP)
- accounting staff, 262–63
- accounts payable vouchers, 209
- adjusting entries, 245, 266, 270
- adverse resulting consequences, 142–43
- aggregate exposure, 72
- AICPA Auditing Standards, 82, 100–102
- American Institute of Certified Public Accountants (AICPA), 68, 77, 82, 85, 97, 99–103
- American Recovery and Reinvestment Act of 2009 (ARRA), xviii
- application(s), 273–83
- application systems, 265–66, 287–88
- ARRA. *See* American Recovery and Reinvestment Act of 2009 (ARRA)

- AS/NZS 4360 standard [Australia and New Zealand], 4, 104–6
- assessment model, 67, 166, 276
- application, 280–83
- control, 70, 109, 303–4, 315
- Excel, 187–88
- quantitative, 179, 201, 306, 311
- summary description, 311–12
- trusted provider, 301–2
- assessment review questions, 314–15
- assumptions, underlying, 23, 28, 30, 237, 262, 265
- attorney-client privilege, 54, 57, 59–61, 63
- audit. *See* insurance model audit law
- accounting policies and procedures, 269
- AICPA Auditing Standards *vs.* COSO-IC, 82
- of computer systems, 125
- of controls, 129
- of control systems, 152
- COSO-IC Model Audit Law, 85
- external, 84
- financial, 148
- independent audit software, 186
- internal, 18, 84, 105, 249, 251–53
- internal audit department, 32
- IRS, 49
- material auditing misstatements, 152
- periodic, 12
- public company, 60, 99
- quantitative approach to, 68
- of risks and controls, 107
- Statements on Auditing Standards (SAS), 78–79, 99–101, 103, 267, 299, 303
- tests, 157, 163, 168, 248
- audit committee, 33, 43, 60, 77, 157, 169, 229, 249, 270
- Sarbanes-Oxley Act*, 319, 321
- auditing procedures, 56–57
- auditing standards, 68. *See also* insurance model audit law
- AICPA Auditing Standards, 82, 100–102
- compliance testing (tests of transactions)*, 234
- Generally Accepted Auditing Standards, 110
- PCAOB's Auditing Standards, 99–100
- Systems Auditability and Control* (SAC), 119, 132, 149
- auditors
- disclosure obligations, 60–61
- external, 59, 72, 100, 102, 110, 135, 203, 249, 252
- internal, 135, 245, 248, 252
- material misstatement in financial statements, 10
- risk assessment, 4, 65
- standard of precision, 13
- Australian/New Zealand (ANZ) Standard for Risk Management, 105–6
- B**
- backup and recovery, 291
- BITS, 104, 109
- business process applications, 273–83
- C**
- Canadian Institute of Chartered Accountants (CICA), 106, 109, 132
- cascading linkage, 200
- chief accounting officers, 248, 258, 262
- CICA. *See* Canadian Institute of Chartered Accountants (CICA)
- CobIT. *See* *Control Objectives for Information and related Technology* (CobIT)
- code of ethics, 266–67
- Committee of Sponsoring Organizations (COSO), 220, 239–42
- communications hardware and software, 289
- company's Charter and bylaws, 58
- competitive analysis, 43–46

- compliance, 5, 13, 23, 32–33, 55,
244–45, 306, 311
- computational errors in applications,
262, 265
- Computer Control Guidelines*, 106
- consent, 61–64
- contingency planning, 21, 291
- continuity of service, 298, 301
- control(s)
- assess the effectiveness of, 139–41
 - characteristics, classification of, 140
 - correction, 187, 279
 - detection, 250, 278–79
 - environment, 242–43
 - evaluation matrix, 143–48
 - functional decision tree, 146
 - group, separate, 248
 - how much is enough/too much?,
148–49
 - implementation, 225–26
 - models, 199–201, 313
 - over controls to assure effective
monitoring, 248–55
 - prevention, 277–78
 - principles and frameworks, 103–4
 - of problems, assess adequacy of,
141–42
 - of problems, relationship of, 141
 - ratings, 306–7
 - redundant or compensating, 250
 - ten selected, 148–49
- control assessment model, 70, 109,
303–4, 315
- control documentation
- accountability, 205
 - activity subject to control, 205
 - AICPA, 100, 204–6
 - description, 206
 - elements of, 204–6
 - identification, 204–5
 - illustration or example, 206
 - integrated database, 315
 - location, 205
 - Microsoft's Office Suite, 211
 - narrative description, 209
 - relationships, 206
 - supervision and review of work,
268
 - trusted systems and, 300
- control frameworks. *See also*
- control(s); COSO-Enterprise Risk
Management (COSO-ERM);
COSO-Internal Control
(COSO-IC); insurance model
audit law
 - adverse resulting consequences,
142–43
 - AICPA, 68, 77, 82, 85, 97, 99–103
 - AS/NZS 4360 standard, 4, 104–6
 - BITs, 104, 109
 - CobiT, 68, 83, 97, 102–4, 193,
285–87, 291
 - CoCo (Canada), 103–4
 - Data Security Standards, 104,
108–10
 - Foreign Corrupt Practices Act of
1977, 75–77, 97
 - holistic risk assessments and ERM,
87, 97
 - IFAC, IASB, and OECD, 106–7
 - International Standard 27002, 104,
107–8
 - managing risk and internal control,
84–86
 - Payment Card Industry (PCI),
108–10
 - PCAOB, 99–100, 103, 111, 227, 240,
303
 - professional standards, 4, 75–84,
99–100, 227, 267
 - recognized, 75
 - risks, organizational, 6, 34, 36, 86,
90, 151
 - shifts from negative to positive
terminology, 147
 - SysTrust, 104, 109–11
 - The Turnbull Report* (U.K.), 104–5
 - Control Objectives for Information
and related Technology* (CobiT),
68, 83, 97, 102–4, 193, 285–87,
291
 - cooperation obligations, 63

- Core Principles for Managing Security of Information, 106
- correction controls, 187, 279
- COSO. *See* Committee of Sponsoring Organizations (COSO)
- COSO-Enterprise Risk Management (COSO-ERM)
- control activities, 95
 - event identification, 93–94
 - framework, 86, 90–97
 - information and communication, 95–96
 - internal environment, 90–92
 - model, 87
 - monitoring, 96
 - objective setting, 92–93
 - overview, 86
 - risk assessment, 94
 - risk components, 90–92
 - risk management objectives, 96–97
 - risk response, 95
- COSO Enterprise Risk Management Framework, 12
- COSO-ERM. *See* COSO-Enterprise Risk Management (COSO-ERM)
- COSO-IC. *See* COSO-Internal Control (COSO-IC)
- COSO-Internal Control (COSO-IC), 12
- about, 77–78
 - control activities, 82–83
 - control components, 80
 - control environment, 80–81
 - five components, 80
 - framework, 91
 - information and communication, 83
 - monitoring, 83–84
 - objectives, 78–80
 - risk assessment, 81–82
- cost of benefits, 72–73
- counterparty feedback, 251
- counterparty treatment, 266, 270
- coverage disputes, 62, 64
- Criteria of Control* (CoCo) [Canada], 103–4
- customer dissatisfaction, 298, 301
- cut-and-paste errors, 184
- D**
- database software, 288
- data entry errors, 182
- data fields and elements, 198
- Data Security Standards (DSS), 104, 108–10 “data | validation” function, 186
- debates, reducing, 72
- defects
- design, 297
 - manufacturing, 297
 - service, 298
- detection without correction, 245
- direction controls, 185–86
- disclosure
- to auditors, 61
 - to government, 60–61
 - inadvertent, 61
 - obligations to auditors, 60
 - to public relations staff, 61
- display formulas for review, 186
- documentation formats, 206–10
- documentation tools, 211–17
- E**
- edit matrices, 209
- electronic security, 290–91
- email, 289–90, 295
- embedded amounts, 182
- Enterprise Risk Management (ERM)
- about, 4, 17–18, 82, 113
 - accountability, emphasizing, 20–21
 - Amazon.com stock returns *vs.* market returns, 24
 - bias, identifying, 22–23
 - black swans, planning for, 21–22
 - failure to communicate, 36–37
 - historical data, trap of, 27–30
 - human element, 35–36
 - IBM stock returns *vs.* market returns, 24
 - inflection points, incorrect, 30–31
 - organizational culture and risk management, 18–20

- risk, analysis of, 23–25
 - risk, issues in managing, 27–37
 - risk management data, 25–27
 - risk management-focused culture, 22–27
 - risk managing in silos, 31–33
 - risks, overlooking, 34
 - S curve with inflection point, 31
 - skewed distribution, sample, 29
 - S&P 500 Index values, 28–29
 - stakeholders' preferences, 25
 - estimates, unreasonable, 265
 - estimation procedures, 51
 - Excel applications
 - annotate responsibility, 187
 - appearance of formal development, 183
 - convert to formal application, 187
 - correction controls, 187
 - cut-and-paste errors, 184
 - data entry errors, 182
 - “data | validation” function, use the, 186
 - direction controls, 185–86
 - display formulas for review, 186
 - embedded amounts, 182
 - environment, 179–80
 - Excel, revise, 187
 - Excel assessment model, 187–88
 - Excel audit software, independent, 186
 - Excel controls, 185–87
 - Excel worksheets, applications of, 180–81
 - figures entered in incorrect formats, 182
 - formulae look to wrong cells, 183
 - formulae reference blank cells, 183
 - guidelines and standards, 185
 - hardcoded values, 182–83
 - incomprehensible design, 183–84
 - logic errors, 184
 - macrocode errors, 184–85
 - misdirected alterations, 185
 - mistaken carryover of data, 184
 - prevention controls, 185
 - program bookkeeping checks, 186
 - recheck sums and calculations, 186
 - review results, 185–86
 - self-reliance, 184
 - “tools | auditing” function, 186
 - “tools | protection” function, 185
 - training, 185
 - what can go wrong with, 181–85
 - external auditors, 59, 72, 100, 102, 110, 135, 203, 249, 252
- F**
- financial accounting process
 - flowchart, 208
 - financial analysis, 40, 43, 50, 251, 261
 - firewalls, 291, 300–301
 - Foreign Corrupt Practices Act of 1977, 75–77, 97
- G**
- GAAP. *See* generally accepted accounting principles (GAAP)
 - game structure, 50–51
 - GASSP. *See* *Generally Accepted System Security Principles (GASSP)*
 - general and infrastructure systems
 - acceptance testing, 290
 - application systems, commercially developed, 287–88
 - application systems, maintenance and changes to, 288
 - application systems, new, 287
 - backup and recovery, 291
 - CobiT for control of IT, 285–87
 - communications hardware and software, 289
 - contingency planning, 291
 - database software, 288
 - electronic security, 290–91
 - email, 289–90
 - environment, 285
 - general systems, control over, 290–91

- general and infrastructure systems
(*Continued*)
- general systems, what can go wrong with, 287–90
 - infrastructure model, 291–93
 - network hardware and software, 289
 - network infrastructure, model of, 292
 - operating system software, 288
 - physical security, 290
 - redundancy, 291
 - supervision, 290
- generally accepted accounting principles (GAAP), 79, 84, 110–11, 221, 252, 257–64
- Generally Accepted Auditing Standards, 110
- Generally Accepted System Security Principles (GASSP)*, 104, 106–7
- general systems
- control over, 290–91
 - what can go wrong with, 287–90
- generic controls, 299
- glossary, 317–18
- H**
- hardcoded values, 182–83
- Health Insurance Portability and Accountability Act (HIPAA), 104
- I**
- IFA. *See* International Federation of Accountants (IFA)
- IIA. *See* The Institute of Internal Auditors (IIA)
- indemnity agreements, 62
- independent ratings, 249
- Information Systems Audit and Control Association (ISACA), 102, 132, 286
- infrastructure model, 194, 291–93
- inherent risks, 72, 83, 86, 94, 125, 138, 154, 246
- Institute of Internal Auditors (IIA), 77, 132
- insurance coverage, 57, 62–63
- insurance model audit law
- about, 110–11, 138
 - cost, 139
 - familiarity, 136–37
 - immediacy, 138
 - independence, 135–36
 - IT responsibility, 134–35
 - location, 132–33
 - mode, 137–38
 - objectives, 131–32
 - objectivity, 131
 - organization, 133–34
 - responsibilities, 134–35
 - who is responsible, 135
- insurance policies, 62–63
- interdependent systems. *See also* control documentation
- accounts payable vouchers, 209
 - applications, 197
 - cascading linkage example, 200
 - consequences spread as problems, 194–98
 - control models, interrelated, 199–201
 - data fields and elements, 198
 - disbursements system flowchart, 212–14
 - documentation formats, common, 206–10
 - documentation tools, 211–17
 - edit matrices, 209
 - financial accounting process flowchart, 208
 - flow charts, 208
 - hierarchy of systems, 198–99
 - interdependencies, 191–92
 - IT infrastructure, dependence on, 192–94
 - linked supporting and dependent systems, 195
 - narrative descriptions, 209
 - risk/control matrices, 209

- risk matrices for field operations, 210
- system and data security, 197
- transactions, 197
- tree chart, 206–7
- internal audit, 18, 84, 105, 249, 251–53
- internal auditors, 135, 245, 248, 252
- internal control assessment
 - about, 219
 - control implementation, 225–26
 - COSO, how does this fit into?, 220
 - internal controls, program for
 - assessment of, 230–32
 - program for, 230–32
 - set ‘S’ is partitioned into subsets A and B, 228
 - step 1: identity and location
 - documented procedures and attributes, 221
 - step 2: prepare documentation of system features, 221–22
 - step 3: list potential problems, 222
 - step 4: consider inherent risks in the control environment, 222
 - step 5: relate control objectives to potential consequences of problems, 223
 - step 6: consider the significance of potential consequences, 223–24
 - step 7: identify and evaluate prevention control activities, 224–25
 - step 8: identify and evaluate detection control activities, 225
 - step 9: identify and evaluate corrective control activities, 225–27
 - step 10: make a preliminary forecast and back test, 227–28
 - step 11: rate the level of control, 228
 - step 12: recalculate consequences and exposure, 228
 - step 13: link the consequences of this system to systems that rely on it, 228–29
 - step 14: consider costs and benefits, 229
 - step 15: test sensitivity, 229
 - step 16: consider potential improvements, 229
 - step 17: prepare a report, 229
 - step 18: selection of key controls for testing, 232–34
 - step 19: derivation of the models, 234
 - step 20: testing procedures, 234–35
 - step 21: reassessment using tested results, 235
 - step 22: interpreting model results, 236–37
 - step 23: remediation and improvement, 237
 - system assessment steps, 220–37
 - verification by testing, 232
 - walkthrough, 227
- internal control monitoring
 - about, 259
 - audit committee, 249
 - compliance, deterioration in control, 244–45
 - compliance, forged or false documentation of, 245
 - compliance only when inspection is anticipated, 245
 - control environment, 242–43
 - control group, separate, 248
 - controls, detection, 250
 - controls, redundant or compensating, 250
 - controls over controls to assure effective monitoring, 248–55
 - COSO monitoring guidance, 239–42
 - counterparty feedback, 251
 - decisive discipline when justified, 253, 255
 - detection without correction, 245
 - disregard of problems by supervisor, 247
 - external auditors, 59, 100, 102, 110, 135, 203, 249, 252
 - financial analysis, 40, 50, 251, 261

- internal control monitoring
 (Continued)
 financial involvement in business activities, 248
 fraud, 247
 independent ratings, 249
 inherent risks, changes in, 246
 internal audit, 251–52
 monitoring activities, periodic, 250–51
 monitoring function under COSO, 255
 monitoring model, example of, 254
 monitoring problems, potential, 243–47
 nature of consequences, change in, 246
 opportunities for problems, changes in volume or value of, 246–47
 other problems, 247
 out-of-system transactions, 244
 periodic management review of problems and all control assessments, 253
 personnel, reliability and competence, 243
 personnel turnover, 243
 potential consequences, 241–42
 problems, change in potential, 246
 problems, potential monitoring, 243–47
 problems, track and compare detected, 250
 problems, upstream reporting of, 253
 problems and weak control assessments, management follow-up of, 253
 regulatory examinations, 252
 segregation of duties, 243
 supervisory review, 249
 system changes, 243
 system internal monitors, 249–50
 time and resource constraints, 242
 whistleblowers, 252
 internal control reporting
 chart perspectives and perception, 305
 control ratings, 306–7
 control ratings, graphical display of, 307
 environment, 303
 incidents, expected, 308
 modeling, results of, 304–9
 problems, nature of the, 306
 quantitative assessment model, 306
 residual incidents, 307–8
 risk, perception of, 304
 total exposure, 308–9
 International Federation of Accountants (IFA), 104, 106
 International Standard 27002, 104, 107–8
 ISACA. See Information Systems Audit and Control Association (ISACA)
- K**
- King Report* [South Africa], 104
- I**
- logic errors, 184
- M**
- macrocode errors, 184–85
 maintenance
 COSO-IC's control activities, 83
 information applications systems, 126–27
 program, 181
 recovery and complex, 121
 scheduled and unscheduled, 301
 systems, 125–26, 135, 199, 203
 by third-party software providers, 100
 mitigating risks in internal investigations and insurance coverage
 about, 53
 analyze the findings, 59

- attorney-client privilege and work product doctrine protection of report, 60–61
 - be independent, 59
 - company's Charter, bylaws and State Employment Regulations, 58
 - consent to defense arrangements, 62–63
 - consent to settlement or payment of judgment, obtain, 63–64
 - cooperation obligations and respond to requests for information and coverage defenses, 63
 - courses of actions, 54–55
 - coverage disputes, resolve, 64
 - deal openly and honestly with employees and other witnesses, 58–59
 - disclosure, inadvertent, 61
 - disclosure obligations to government and company's auditors, 60
 - disclosure to auditors, 61
 - disclosure to government, 60–61
 - disclosure to public relations staff or government affairs consultants, 61
 - insurance coverage, maximize the potential, 62–63
 - insurance policies or indemnity agreements, gather relevant, 62
 - investigation and analysis of results, carrying out, 58–61
 - lessons learned for renewal, consider, 64
 - message and priorities communication, 65
 - notice of claims or potential claims to primary and excess insurers, 62
 - plan development, 57–58
 - plan to ameliorate deficiencies contributing to the problem, 64–65
 - plan to correct deficiencies and remediate harm, 62–65
 - reform, measure effectiveness of, 65
 - risks, assess the, 55–57
 - root causes, assessing, 55, 64
 - scenario, 53–54
 - self-critical analysis, privilege of, 61
 - systems or contributing causes, fixing, 64–65
 - modeling
 - application assessment, 280–82
 - basic modeling concept, 312–14
 - concept, basic, 312–14
 - control, 153
 - errors, 179
 - infrastructure, 291–93
 - internal control reporting, 304–9
 - network infrastructure, 292
 - quantitative, 73, 152, 239, 315–16
 - quantitative assessment model, 311–12
 - results of, 304–9
 - scalable risk assessment, 67
 - validity of, 70–71
- N**
- network hardware and software, 289
 - network infrastructure model, 292
 - number controls, 162
- O**
- OECD. *See* Organization for Economic Cooperation and Development (OECD)
 - operating controls, 300
 - operating system software, 285, 288
 - operational risk mitigation by strategic thinking
 - about, 39
 - competitive analysis, 43–46
 - estimation procedures, 51
 - game structure, revised, 51
 - risk mitigation by strategic behavioral analysis, 41–43
 - scorecard for analysis of current market players, 46–48

- scorecard for evaluating current market players, 47
 - sports analogy, 40–41
 - strategic behavior, 39–40
 - strategic decisions of firms A and B, 42
 - strategic risks, quantification of, 50–51
 - unpredictability, benefits of, 48–50
 - operations documentation, 299
 - organizational risk management
 - about, 1–4
 - CFOs, top concerns of U.S., 3
 - risk assessment process, 4–5
 - risk management, 5–7
 - strategy, goals of, 11
 - U.S. goods and services foreign trade deficit, 3
 - Organization for Economic Cooperation and Development (OECD), 104, 106–7
- P**
- password rotation, 300
 - Payment Card Industry (PCI), 108–10
 - Payment Card Industry Data Security Standards* (PCI DSS), 104
 - PCAOB. *See* Public Company Accounting Oversight Board (PCAOB)
 - PCAOB's Auditing Standards, 99–100
 - personnel selection, 266–67
 - Pervasive Principles of Generally Accepted Security Principles, 106
 - physical security, 290
 - Principles for Guidelines for the Security of Information Systems, 106
 - problems
 - change in nature of potential, 246
 - potential monitoring, 243–47
 - track and compare detected, 250
 - upstream reporting of, 253
 - and weak control assessments, 253
 - professional standards, 4, 75–84, 99–100, 227, 267
 - provider
 - assessment model of trusted, 301
 - model of trusted, 302
 - problems, 297–98
 - service, 65, 109, 191
 - software, third-party, 199
 - stability, evaluate, 299
 - Public Company Accounting Oversight Board (PCAOB), 99–100, 103, 111, 227, 240, 303
- Q**
- quantitative assessment model, 179, 201, 306, 311
 - quantitative control relationships
 - about, 151
 - “anyone can build a model,” 173–75
 - control environment risk calculations, 159
 - input 1: potential problems (incidents), 153
 - input 2: opportunities, 154
 - input 3: inherent risk factors, 154–56
 - input 4: control environment, 157–59
 - input 5: prevention controls, 160–62
 - input 6: implementation of controls, 162–63
 - input 7: detection controls, 164–65
 - input 8: correction controls, 166–68
 - input 9: control costs, 169–70
 - input 10: consequences, 170–71
 - input 11: loss value per incident, 171
 - model, example of simple, 174
 - number controls, impact of overestimation by, 162
 - output A: forecast actual incidents, 164
 - output B: forecast detected incidents, 165–66

- output C: forecast residual incidents, 168
 - output D: control ratings, 169
 - output E: constraints and limitations, 173
 - output E: exposure, 171–73
 - output E: exposure calculations, example of, 172
 - output E: probability distribution of consequences, 173
 - precision of results, 175–76
 - qualitative to quantitative, moving from, 151–52
 - residual problems, consequences of, 170
 - results, precision of, 175–76
 - results, sensitivity of, 176–77
 - risk, correction control, 167
 - risk, prevention control, 163
 - risk, residual, 169
 - risk and potential incidents, preliminary, 159–73
 - risk calculation, example of inherent, 156
 - risks, detection control, 166
 - systems control functions, 152–59
 - quantitative estimation methods, 266, 268
 - quantitative risk management
 - about, 67–68
 - aggregate exposure, 72
 - benefits, cost of, 72–73
 - debates, reducing, 72
 - documenting for review, 71
 - financial objectives, focusing on, 71
 - modeling, validity of, 70–71
 - multiple instances, 72
 - risk, predicting residual, 69–70
 - sensitivity and “what-if” analysis, performing, 71
 - subject-matter experts, collaborating with, 70
 - why is a quantitative approach important?, 68–73
- R**
- redundancy, 250, 291
 - reference literature, 266–67
 - regulatory examinations, 252, 266, 269
 - residual incidents, 168–69, 194, 236, 283, 307–8
 - results
 - precision of, 175–76
 - sensitivity of, 176–77
 - review and acceptance assessments
 - assessment model, summary of, 311–12
 - assessment review, questions for, 314–15
 - control model, 313
 - modeling concept, basic, 312–14
 - risk(s)
 - assessment process, 4–5
 - assessments, influences in, 14–16
 - assessments and ERM, holistic, 87, 89
 - assess the, 55–57
 - bias, 16
 - calculation, example of inherent, 156
 - control matrices, 209
 - correction control, 167
 - definition of, 9–11
 - detection control, 166
 - evaluation, 12
 - identification, 11
 - information, quality of, 14–15
 - inherent, 72, 83, 86, 94, 125, 138, 154, 246
 - internal control and, managing, 84–86
 - management, importance of proper, 6–7
 - management at the board level, 5
 - management engagement, scope of, 13–14
 - management strategy, 11–13
 - matrices, field operations fiscal year 20X3, 210
 - mitigation, 12–13

- risk(s) (*Continued*)
- mitigation by strategic behavioral analysis, 41–43
 - organizational, 6, 34, 36, 86, 90, 151
 - perception of, 304
 - potential incidents and, preliminary, 159–73
 - potential problems in a
 - manufacturing setting, 11
 - prevention control, 163
 - professional judgment, 14
 - quantification of strategic, 50–51
 - residual, 169
- root causes, 55, 64
- S**
- Sarbanes-Oxley Act, 4, 33, 68, 78, 104–5, 157, 219, 239, 253, 319–22
- Sec. 301: Public Audit Committees, 319–20
 - Sec. 302, 320–21
 - Sec. 404: Management Assessment of Internal Controls, 321
 - Sec. 407: Disclosure of Audit Committee Financial Expert, 321–22
- SAS. *See* Statements on Auditing Standards (SAS)
- scorecard, 44–48
- security, system and data, 197
- segregation of duties, 243
- self-critical analysis, 61
- sensitivity and “what-if” analysis, 71
- side agreements, incomplete, 263
- State Employment Regulations, 58
- Statements on Auditing Standards (SAS), 78–79, 99–101, 103, 267, 299, 303
- Statutory Accounting Principles* (SAP), 111, 259
- strategic behavior, 39–40
- strategic decisions of firms A and B, 42
- strategic risks quantification, 50–51
- subject-matter experts, 70
- supervision, 268, 290
- supervisory review, 249
- system assessment steps, 220–37
- system changes, 243
- system internal monitors, 249–50
- system providers, trusted
- acceptance tests, 301
 - continuity of service, 298
 - customer dissatisfaction, 298, 301
 - defects, design, 297
 - defects, manufacturing, 297
 - defects, service, 298
 - environment, 295
 - firewalls, 291, 300–301
 - generic controls, 299
 - how much to trust trusted systems?, 296
 - internal controls over trusted systems, 298–301
 - maintenance, scheduled and unscheduled, 301
 - operating controls, typical, 300
 - operations documentation, 299
 - password rotation, 300
 - post-implementation reviews, 301
 - provider problems, 297–98
 - provider stability, evaluate, 299
 - strong contracts and service-level agreements (SLAs), 299
 - third-party control attestation reports, 299–300
 - trusted provider assessment model, 301
 - trusted provider model, example, 302
 - user operating errors, 298
- Systems Auditability and Control* (SAC) study, 119, 132, 149
- systems control functions, 152–59
- SysTrust, 104, 109–11
- T**
- third-party control attestation reports, 299–300
- time and resource constraints, 242
- “tools | auditing” function, use,

186 “tools | protection” function,
185
total exposure, 308–9
training and education, 268
transactions, misclassified, 265
tree chart, 206–7
Turnbull Report, 4, 103–5

U

unpredictability, benefits of, 48–50

user operating errors, 298

V

verification by testing, 232

W

walkthrough, 227
whistleblowers, 252, 269
written communication, 267–68

<http://www.pbookshop.com>

<http://www.pbookshop.com>