

Index

A

Accountability, 55
Accounting for internal controls, 55
Acquisition, development, and maintenance processes, 81
AICPA developed processes, 285
AICPA SAS No. 1, 5
AICPA's Auditing Standards Board (ASB), 16
American Institute of Certified Public Accountants (AICPA), 6
Analyst conflicts of interest, 26
Andersen Consulting, 26
Application controls, 76
Application records management reporting controls, 148
Audit committees, 183, 278, 279
Auditing practices for external auditors, 16
Auditing Standard No. 5 (AS No. 5), 114
Auditor independence, 18
Authority and responsibility management requirements, 49
Authorizations and approvals, 76
Availability management objectives, 198

B

Basic principles that support enterprise COSO internal controls, 31
Benchmarking and peer evaluations, 112
Board of directors committees, 276
decisions, 272

responsibilities, 271, 273, 278, 281, 282
risk oversight responsibilities, 278
role, 48
senior management reporting, 113
Budget function interactions, 122
Budgeting processes, 121
Budget performance monitoring, 121
Budget planning processes, 120
Business operations internal controls, 39
Business processes, 76
Business unit-level documented procedures, 179

C

Changes in the new revised COSO framework, 36, 38
Chief compliance officer roles, 157
Client-server architecture, 189
Client-server general controls, 188
Cloud computing, 128, 208, 210, 215
internal controls, 211
Cloud service providers, 211
COBIT, 241, 245, 250, 253, 255
enablers, 249
general architecture, 248, 249
objectives mapping, 255
Principle 1, 246
Principle 2, 246
Principle 3, 247
Principle 4, 249
Principle 5, 252
Principles, 245, 248
Code acknowledgments, 46

- Codes of conduct, 44, 171
- Codes of ethics, 25
- Cohen Commission, 9
- Commitment to competence, 52, 53
- Committee of Sponsoring Organizations (COSO), 12
- Communication
 - concepts, 89
 - to external parties, 100
 - of monitoring findings, 113
- Compliance Prevention and Remediation Programs, 159
- Concepts and definitions, 88
- Continuous monitoring, 109
 - processes, 108
- Control activities, 73, 76, 80, 233
 - objectives, 76, 77
 - principles, 74, 78, 83, 85
- Control environment, 41
 - internal control concepts, 41
 - internal controls, 42
 - principles, 43, 44, 48, 49, 51, 52, 54, 55
 - supporting principles, 57
- Controls over internal reporting
 - processes, 39
- Corporate and management goals, 120
- Corporate audit committee
 - charters, 280
- Corporate audit records, 27
- Corporate boards of directors, 271, 276, 280
- Corporate charters, 276
- Corporate fraud accountability, 27
- Corporate mission statements, 170
 - examples, 226
- Corporate responsibility, 20
- COSO
 - commitment to competence, 53
 - control activities, 81, 85
 - enterprise communication, 87
 - ERM, 59, 68, 240
 - ERM components, 223, 225, 227, 228, 229, 233, 236
 - ERM framework, 217, 219, 220, 221, 232, 237, 238
 - model, 222
 - framework changes, 32, 36
 - GRC perspective, 118
 - information and communication, 87, 88, 89, 95, 97
 - internal control, 31, 36, 182, 183, 186, 200, 204, 208, 234, 271
 - components, 41, 59, 73, 74, 75, 78, 87, 90, 105, 108
 - framework, 59, 73, 118, 133, 137, 141, 153, 155, 157, 158, 159, 161, 162, 163, 166, 168, 175, 178, 179, 181, 183, 193, 214, 217, 256, 269, 271, 285, 288
 - framework definition, 88, 89
 - original framework, 13, 31
 - principles, 38
 - processes, 117, 213, 286
 - pyramid view, 31
 - reporting, 143, 146, 148, 149, 157, 165
 - internal financial reporting
 - controls, 141
 - IT-related goals, 253
 - monitoring
 - principles, 108
 - processes, 105, 106, 108, 110, 112, 114, 115
 - objectives, 39, 57, 60
 - operations
 - controls, 118, 121, 123
 - objectives, 118, 126, 130
 - policy and governance controls, 123
 - published guidance materials, 40
 - reporting
 - objectives, 137, 138, 140, 142
 - requirements component, 137
- risk
 - objectives, 60, 62, 66, 67
 - response strategies, 67, 68, 69, 70

- Covering end to end enterprise goals, 246
- Customer service feedback, 100
- D**
- Deming PDCA quality cycle, 95
- Department and unit level internal controls, 178
- Division and functional unit internal controls, 175
- Document imaging processes, 143
- Document library service technologies, 144
- Document-management systems, 150
- E**
- EDMS technology components, 142
- Effective budgeting systems, 119
- Effective GRC principles, 271
- Effective internal control systems, 139
- Electronic document management systems (EDMS), 141, 143
- Enabler process goals, 246
- Enhanced financial disclosures, 23
- Enron, 26
 - audit committee failures, 279
- Enterprise
 - business risks, 63, 65
 - codes of conduct, 44, 46, 47
 - compliance
 - activities, 168, 169
 - controls, 153
 - direct supervision, 109
 - document-reporting internal controls, 146
 - external communications, 100, 102
 - governance, 240
 - components, 2
 - elements, 167, 169, 172, 175
 - internal controls, 165, 170, 171
 - principles, 165
 - human resources function, 52
 - information systems quality requirements, 93
 - internal
 - communications, 96
 - controls, 253
 - management responsibilities, 141
- Enterprise risk management (ERM), 217, 222
 - definition, 220
- Enterprise-specific control activity factors, 75
- ERM (enterprise risk management) control activities, 238
- Establishing effective internal controls, 33, 286
- Evaluating internal control deficiencies, 112
- Event identification risk management components, 227
- External communications, 100, 101
 - processes, 87
- External financial reporting, 30, 33
 - controls, 139
 - internal controls, 140
 - objectives, 33, 138, 139
- External nonfinancial reporting internal controls, 149
- External risk factors, 65
- F**
- FCPA (Foreign Corrupt Practices Act), 7
- Financial and nonfinancial reports, 137
- Financial Executives International (FEI), 9
- Financial management for IT services, 194
- Financial reporting
 - controls, 139, 141
 - policies, 140
 - requirements, 138
- First-level supervision, 110
- Foreign Corrupt Practices Act (FCPA), 7, 9
- Forms management internal controls, 148, 150

- Fraud
 - accountability and white-collar crime, 26
 - detection, 70
 - risk analysis, 69
- Fraudulent reporting risks, 70
- G**
- General counsel responsibilities, 157
- Generally accepted accounting principles (GAAP), 17
- Goal setting and planning, 120
- Governance, 252
 - best practices, 167
 - tools, 134
- Governance, risk, and compliance (GRC)
 - policies, 84, 117
 - concepts, 163, 164
 - operations controls, 117
 - principles, 273
 - risk management, 166, 167
- Governmental and other regulatory reports, 139
- Graphical user interfaces (GUI), 145
- Guidance materials changes, 32
- H**
- Higher-priority risks, 110
- Human resources policies and practices, 51, 52, 53, 54
- I**
- Implementing internal controls
 - processes, 293
- Implementing the new COSO
 - framework, 296
- Inbound communications, 100
- Information and communication, 87, 92
 - components, 236
 - concepts, 88
 - flows, 237
 - principles, 89, 96, 100
 - processing objectives, 76
 - requirements, 90
- Information systems, 93
- Inherent risk, 66, 227
- Integrated internal control architecture
 - frameworks, 247
- Integrated technology-enabled processes, 93
- Integrity and ethical values, 43
- Internal audit
 - evaluations, 108
 - outsourcing, 18
 - reports, 113
 - responsibilities, 110
- Internal communications, 96
 - processes, 87
- Internal Control—Integrated Framework, 12, 40
- Internal controls, 3
 - assessments, 24
 - auditing standards, 10, 16, 17, 287
 - communication, 95, 96
 - compliance objectives, 34
 - definition, 3, 5, 6, 7, 9, 10, 13, 30
 - GRC issues, 161
 - individual responsibilities, 54, 55
 - knowledge requirements, 282
 - legal issues, 157
 - limitations, 292
 - management, 282
 - objectives, 39, 53, 89
 - policies and procedures, 83, 84
 - principles, 294
 - processes, 2, 272, 278
 - quality audits, 95
 - requirements, 7, 10, 14
 - responsibilities, 98, 294
 - risks, 204
- Internal environment risk management
 - elements, 223, 224
- Internal reporting objectives, 33
- Internal risk factors, 65
- International Standards Organization (ISO)
 - background, 259
 - documentation hierarchy, 265
 - internal control, 259
 - international standards, 158

- ISO 2000, 268
 - ISO 27002, 266
 - ISO 9001 quality management systems, 262
 - IT security standards, 266
 - service quality management standards, 268
 - standards, 262, 265, 269
 - Information technology (IT)
 - application controls, 130, 131, 210
 - applications development review guidelines, 132
 - audit function management, 185
 - automated monitoring, 110
 - availability-and-costs relationships, 199
 - controls hierarchy, 183
 - documentation, 126
 - general and application internal control processes, 191, 192
 - general controls, 78, 79, 80, 181
 - general controls definitions, 79
 - governance, 125
 - general controls, 183
 - policies and practices, 125
 - infrastructure controls, 182
 - internal controls, 192, 215
 - issues, 131
 - management
 - general controls, 185, 188
 - and organization controls, 125, 126, 129
 - requirements, 134
 - operating systems architecture, 130
 - operations, 189
 - control hierarchy, 123
 - internal controls, 197
 - physical and environmental general controls, 127, 128, 186
 - security
 - internal control issues, 81
 - and privacy, 212
 - requirements, 266
 - standards, 125
 - service
 - bureaus, 287
 - catalogs, 134
 - management, 192
 - procedures catalog, 175
 - standards, 125, 185
 - systems
 - development application controls, 130
 - operational controls, 119, 123
 - software controls, 129, 130
 - technology access rights, 81
 - wireless networks, 204, 207
 - Information Technology Infrastructure Library (ITIL)
 - availability management, 198, 199
 - best practices, 192, 193, 194, 197, 198
 - capacity management, 197
 - service delivery, 196
 - best practices, 200
 - service management, 191, 196
 - IT Governance Institute, 241
 - IT-related internal control considerations, 85
 - IT-related management and operations, 125
- J**
- Johnson & Johnson Tylenol crisis, 169
- K**
- Key components of internal control, 36
- L**
- Launching enterprise monitoring processes, 115
- M**
- Major components of internal control, 31
 - Management assessment of internal controls, 24
 - Managing internal controls, 279
 - Mapping COBIT, 256
 - Materiality financial reporting concepts, 61

- Meeting stakeholder needs, 246
 - Methods of communication, 98
 - Mission statements, 169
 - codes of conduct, 224
 - Monitoring activities, 105
 - principles, 106, 112
 - Monitoring
 - components, 238
 - internal control procedures, 115
- N**
- National Commission on Fraudulent Reporting, 12
 - Negative assurance, 10
 - Nonfinancial reports and processes, 39
- O**
- Objective-setting, risk management
 - components, 225, 226
 - Officer disclosure sign-off statements, 20
 - Ongoing evaluation processes, 109
 - Operating and financial budgets, 121
 - Operations
 - controls, 119, 120, 122, 127
 - objectives, 118
 - procedures, 133
 - Organizational charts, 51
 - Organization-level internal controls, 162
 - Original COSO framework, 12, 13
 - Outside service providers, 102
 - Outsourced service providers, 112
 - Overlapping internal control
 - categories, 40
 - objectives, 35
- P**
- Password control systems, 81
 - PCAOB (Public Company Accounting Oversight Board), 14, 16
 - Performance measures, 55
 - Physical controls, 76
 - Planning
 - budgeting, 119
 - preparing for personnel succession, 54
 - Portfolio views of risk, 219
 - Professional standards compliance, 158
 - Public Company Accounting Oversight Board (PCAOB), 14, 16
- Q**
- Quality
 - information, 93
 - management system processes, 265
 - review and improvement processes, 95
- R**
- Reconciliations, 77
 - Records information management (RIM)
 - processes, 148
 - Records life-cycle processes, 148
 - Regulatory
 - compliance internal control issues, 155, 156
 - compliance reviews, 100
 - public policy committees, 156
 - Reporting
 - control workflow technologies, 145
 - external nonfinancial information, 138
 - objectives, 137
 - Residual risk, 66, 228
 - Responsibilities for preparation and delivery of accurate financial reports, 139
 - Responsibility reporting, 121
 - Revised COSO internal control
 - framework, 82, 87, 293, 294, 295, 296
 - framework changes, 32
 - internal control framework, 30, 32, 33, 34, 35, 36, 38, 40, 41, 240
 - Right-to-audit clauses, 290
 - Risk
 - acceptance, 67
 - appetite, 68, 164
 - concepts, 221

- assessment, 59, 63
 - components, 227
 - factors, 42
 - integration, 74, 75
 - principles, 60, 61, 62, 65, 66, 68
 - process steps, 66
- avoidance, 67
- identification and analysis, 62
 - processes, 62
- likelihood, 229
- management, 70
 - definition, 60
 - philosophy, 223
 - standards, 259
 - strategies, 67
- mitigation, 75
- ranking methods, 219
- reduction, 67
- related events, 234
- response planning, 232
- response strategies, 229, 230
- sharing, 67
- tolerance, 70, 230
- velocity, 65

S

- Software as a Service (SaaS)
 - applications, 212, 213
 - controls, 211
- Sarbanes Oxley Act (SOx), 14, 16
 - audit partner rotation, 20
 - requirements, 171, 281
- Section 404 internal controls
 - evaluations, 132
- Titles
 - II, 18, 20
 - III, 20
 - IV, 23
 - V, 26
 - VI, 27
 - XI, 27
 - VI through X, 26
- whistleblower responsibilities, 97

- Section 404, 24
 - requirements, 24, 25
- Security management processes, 76, 81
- Self-assessments, 112
- Separate and ongoing monitoring
 - evaluations, 108
- Separate monitoring evaluations, 110
- Separating governance from
 - management, 252
- Service catalogs, 133
- Service delivery
 - availability management, 198
 - capacity management, 197
- Service level agreements (SLAs), 196
 - processes, 197
- Service management, 181
- Service Organization Control (SOC)
 - reports, 112, 285, 286, 288, 290, 292
- Service organizations, 286
- Service strategies, 194
- Significant internal review changes, 293
- Smaller IT systems operations, 128
- SOC reporting decision processes, 290
- Software as a Service (SaaS), 210
- Standing data controls, 76
- Statements of Auditing Standards (SAS)
 - SAS 70, 287
 - SAS 99, 69
 - SAS No. 55, 10
 - SAS No. 78, 10
- Storage management virtualization, 214
- Strategic planning, 120
- Supervisory controls, 76
- Systems development life cycle (SDLC)
 - processes, 82
 - standards, 125, 132, 185

T

- Technology general controls, 78, 80, 81, 82
 - infrastructure, 80
- Tone at the top, 41, 43, 169

Transaction

- accuracy, 76
- completeness, 76
- control activities, 76, 77
- controls, 76
- transitioning rules, 295
- Treadway Commission, 9, 12
- validity, 77

V

- Verifications, 77
- Violations and corrective actions, 47

Virtualization, 214

- Virtualization concepts, 215

W

Whistleblower facilities, 47

Wireless

- network vulnerabilities,
207, 208
- security, 208
- system routers, 206

Workflow functionality

- processes, 145

<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>