

Index

A

- Application portfolios, IT portfolio management, 260
- Application systems development, 264
 - enterprise resource planning (ERP) systems, 264
 - ERP systems, 264
 - rapid application development (RAD), 267
 - systems development life-cycle (SDLC) processes, 264
- AS5, risk-based approaches, 27
- AS5 rules, Section 404 internal controls assessments, 17
- Assignment of authority and responsibility, COSO control environment components, 56
- Audit committee internal control issues, IT governance, 375
- Audit committees
 - IT governance responsibilities, 374
 - SOx rules, 23, 372
- Audit evidence classifications, internal audit processes, 328
- Auditor Independence, Sarbanes-Oxley Act (SOx), 18
- Availability management, ITIL service strategy processes, 96

B

- Basic accounting cycles, Section 404 internal controls assessments, 15
- Benchmarking, internal control evaluation processes, 62

- Best practices standards for IT service support, 288
- Board of directors and audit committee
 - COSO control environment components, 55
 - IT governance, 371
- Business Continuity Plan (BCP) Life Cycle, IT governance, 190
- Business continuity planning (BCP)
 - BCP standards, 189
 - disaster recovery planning, 188
 - IT governance, 188
 - IT security practices, 192
- Business continuity planning (BCP) standards, 189
- Business performance, IT Governance Concepts, 6

C

- Capacity management, ITIL service strategy processes, 95
- CEO financial report certification
 - criminal penalties, 24
 - officer disclosure sign-off, 24
 - Sarbanes-Oxley Act (SOx), 23
- Change management processes, IT governance, 100
- Charging for IT services, ITIL financial management, 94
- Client-server systems applications development, 268
- Cloud computing application controls
 - IT application controls, 164
 - SAS 70, 164

- Cloud computing concepts, 164
 - IT governance and assurance issues, 165
 - security and privacy challenges, 166
- Cloud computing data location issues, IT governance concerns, 167
- Cloud computing data segregation, IT governance concerns, 167
- Cloud computing descriptions, IT concepts, 162
- Cloud computing investigative support, IT governance concerns, 167
- Cloud computing IT governance and assurance issues, cloud computing concepts, 165
- Cloud computing long-term viability issues, IT governance concerns, 167
- Cloud computing recovery issues, IT governance concerns, 167
- Cloud computing regulatory compliance, IT governance concerns, 167
- CMDB. *See* Configuration management database
- COBIT
 - COSO internal control framework, 71
 - ISO 38500 principles, 119
 - IT Governance Institute (ITGI), 68
 - IT governance principles, 70
 - IT-oriented internal control assessments, 67
 - SOx internal controls requirements, 71, 84
 - SOx Section 404, 84
 - Val IT best practices governance framework, 298
- COBIT governance objectives
 - enterprise goals, 76
 - governance definition, 81
- COBIT financial governance objectives, enterprise goals, 77
- COBIT 5 simplified general architecture, IT architecture enablers, 73
- COBIT internal stakeholder needs, 74
- COBIT IT security guidance, IT security model concepts, 185
- COBIT principles
 - IT architecture enablers, 72
 - IT governance and management, 80
 - IT governance value objectives, 75
 - IT risk management enablers, 78
- COBIT processes, management of enterprise IT, 81
- COBIT strengths, IT governance focus, 85
- COBIT enablers
 - enabler concepts, 80
 - types of, 79
- Code of conduct stakeholder communications, enterprise codes of conduct, 344
- Code violations and corrective actions, enterprise codes of conduct, 345
- Codes of ethics, Senior Financial Officer SOx requirements, 26
- Commitment to competence, COSO control environment components, 55
- Communications and information, COSO internal control framework, 59
- Compliance internal controls, COSO internal control framework, 53
- Computers at risk (CAR), U.S. National Research Council, 179
- Configuration management database (CMDB), processes, 102
- Configuration management database (CMDB) components
 - conceptual view, 256
 - configuration items (CIs), 252
 - database configuration management facilities, 255
 - database federation, 257
 - data integration and management repositories, 255
 - data synchronization, 258
 - IT configuration management systems, 247
 - ITIL transition management processes, 101
 - security and data protection controls, 255
 - security and user access tools, 255

- Configuration management definition, IT configuration management concepts, 249
- Conflict-of-interest provisions, Sarbanes-Oxley Act (SOx), 26
- Constant improvements program, GLBA Safeguards compliance, 206
- Continuity management, ITIL service strategy processes, 98
- Control activities
 - COSO Internal Control Framework, 57
 - functional or activity management, 58
 - information processing, 58
 - performance indicators, 58
 - physical controls, 58
 - segregation of duties, 58
 - top-level reviews, 58
- Control environment, COSO internal control framework, 54
- Corporate ethics, IT governance concepts, 9
- Corporate responsibilities, Sarbanes-Oxley Act (SOx), 22
- COSO, COSO internal control framework, 53
- COSO, National Commission on Fraudulent Financial Reporting, 52
- COSO components and COBIT
 - objectives, mapping IT governance relationships, 85
- COSO control environment, tone at the top, 54
- COSO control environment components
 - assignment of authority and responsibility, 56
 - board of directors and audit committee, 55
 - commitment to competence, 55
 - human resources policies and procedures, 56
 - integrity and ethical values, 55
 - management philosophy and operational style, 55
 - organizational structure, 56
- COSO enterprise risk management (ERM) framework, IT governance concepts, 30
- COSO ERM
 - control activities, 149
 - documentation, 148
 - enterprise risk management, 134
- COSO ERM framework
 - control activities, 148
 - event identification, 141
 - information and communication, 149
 - internal environment, 138
 - risk responses, 145
 - monitoring, 151
 - objective setting, 140
 - risk appetite, 135
 - risk appetite map, 139
 - risk assessment, 144
 - risk management philosophy, 138
- COSO ERM monitoring
 - framework, 151
 - process flowcharting, 152
 - risk monitoring activities, 151
- COSO ERM risk event–risk response activities, 147
- COSO internal control framework
 - COBIT, 71
 - communications and information, 59
 - compliance internal controls, 53
 - control activities, 57
 - control environment, 54
 - COSO, 53
 - definition, 49
 - dimensions of all internal controls, 64
 - financial reporting internal controls, 53
 - foundation components, 60
 - impact on IT governance, 54
 - importance of COSO internal controls, 66
 - internal controls definition, 53
 - internal control evaluation processes, 62
 - IT audit guidance, 68
 - IT governance guidance, 68
 - IT governance objectives, 49

- COSO internal control (*continued*)
 - IT-related internal controls, 50
 - monitoring, 60
 - monitoring guidance, 65
 - operations internal controls, 53
 - risk assessment, 57
 - standards background, 51
 - Treadway Commission, 52
- COSO monitoring design and implementation process, internal control evaluation processes, 65
- COSO risk assessment processes, internal control framework, 57
- Costs and benefits, IT security, 180
- Criminal penalties, CEO financial report certification, 24
- Cryptography, HIPAA security requirements, 211
- D**
- Database configuration management facilities, CMDB components, 255
- Database federation, CMDB components, 257
- Data management database repository, CMDB components, 255
- Definition of internal control
 - internal control standards background, 51
 - SAS No. 1, 51
- Definition of IT governance
 - IT governance concepts, 29
 - IT governance objectives, 30
- Deming, Edward M., quality management standards, 112
- Design-time policies, IT service-oriented architecture (SOA), 240
- Design-time SOA processes, SDLC processes, 240
- Dimensions of all internal controls, COSO internal control framework, 64
- Disaster recovery planning
 - business continuity planning, 188
 - IT continuity planning, 187
- Document archiving, ECM features, 313
- Document classification processes, ECM features, 315
- Document governance management, ECM features, 316
- E**
- ECM architecture, IT governance, 313
- ECM concepts, IT applications internal controls, 310
- ECM features
 - document archiving, 313
 - document classification processes, 315
 - document governance management, 316
- ECM processes, IT governance, 310
- ECM security tools, IT security processes, 313
- Effective risk management programs, GRC concepts, 40
- Enabler concepts, COBIT types of enablers, 80
- Enron failure, IT governance issues, 9
- Enterprise business risks, risk management fundamentals, 129
- Enterprise codes of conduct
 - code of conduct stakeholder communications, 344
 - code violations and corrective actions, 345
 - IT governance, 341
 - whistleblower and hotline functions, 346
- Enterprise compliance challenges, GRC compliance, 42
- Enterprise compliance issues, government rules and laws, 37
- Enterprise compliance scope, GRC compliance, 44
- Enterprise content management (ECM), IT governance, 309
- Enterprise ethics, IT governance, 337
- Enterprise ethics hotline functions, IT governance, 350
- Enterprise goals

- COBIT governance objectives, 76
 - COBIT financial governance objectives, 77
 - Enterprise governance, ethics programs, 352
 - Enterprise governance concepts, GRC Principles, 40
 - Enterprise governance issues, IT governance, 28
 - Enterprise IT governance goals, IT governance concepts, 7
 - Enterprise organization issues, IT governance concepts, 32
 - Enterprise resource planning (ERP) systems
 - application systems development, 264
 - ERP objectives and requirements, 271
 - ERP system configuration, 270
 - tangible and intangible ERP system benefits, 272
 - Enterprise risk management, COSO ERM, 134
 - Environmental risk analysis, GLBA safeguards compliance, 206
 - ERM components, information and communication flows, 150
 - ERP system configuration, 270
 - ERP systems, application systems development, 264
 - Ethical standards, SOX compliance processes, 27
 - Ethical workplace cultures, IT governance, 337
 - Ethics programs, enterprise governance, 352
 - External auditor, internal controls review requirements, Section 404 internal controls assessments, 19
 - External audit partner rotation, Sarbanes-Oxley Act (SOx), 21
- F**
- Facebook, social media system examples, 358
 - Facebook, using, 359
 - Federal whistleblower rules, whistleblower and hotline functions, 348
 - Financial management for IT services, ITIL service strategy components, 93
 - Financial management of IT systems, IT governance, 95
 - Financial privacy rules, Gramm-Leach-Bliley Act (GLBA), 204
 - Financial reporting internal controls, COSO internal control framework, 53
 - Functional or activity management, control activities, 58
- G**
- GASSP, implementing IT security principles, 183
 - GASSP body of knowledge, IT security standards, 184
 - GASSP principles, IT security purposes, 179
 - Generally accepted system security principles (GASSP), IT security standards, 179
 - GLBA, IT security standards, 203
 - GLBA Pretexting Rules, 206
 - GLBA Safeguards compliance
 - constant improvements program, 206
 - environmental risk analysis, 206
 - monitoring and auditing, 206
 - GLBA safeguards rule, Gramm-Leach-Bliley Act (GLBA), 205
 - Governance definition, COBIT governance objectives, 81
 - Governance, risk and compliance issues, GRC Principles, 38
 - Governance, risk, and compliance processes, IT governance, 45
 - Government rules and laws, enterprise compliance issues, 37
 - Gramm-Leach-Bliley Act (GLBA)
 - financial Privacy Rules, 204
 - GLBA Safeguards Rule, 205
 - IT governance rules, 205
 - IT privacy legislation, 203

- Gramm-Leach-Bliley (*continued*)
 IT security standards, 203
 pretexting, 203
- GRC capability model, OCEG Red Book, 292
- GRC capability model elements, Open Compliance and Ethics Group (OCEG), 293
- GRC compliance
 enterprise compliance challenges, 42
 enterprise compliance scope, 44
 risk management overview, 42
- GRC concepts, effective risk management programs, 40
- GRC governance elements, IT governance concepts, 41
- GRC guidance, Open Compliance and Ethics Group (OCEG), 292
- GRC principles
 enterprise governance concepts, 40
 governance, risk, and compliance issues, 38
 IT Governance Concepts, 39
- H**
- Health Insurance Portability and Accountability Act (HIPAA), IT privacy rules, 208
- HIPAA
 IT governance requirements, 212
 IT privacy rules, 208
 IT security administrative procedures, 213
- HIPAA patient record privacy rules
 IT privacy rules, 209
 medical records disclosures, 210
- HIPAA security requirements
 cryptography, 211
 security services and mechanisms, 214
- Human resources policies and procedures, COSO control environment components, 56
- I**
- Impact of social media computing
 IT governance, 365
 IT system risks, 365
 social media systems, 364
- Impact on IT governance, COSO internal control framework, 54
- Implementing IT configuration management, IT governance, 253
- Implementing IT security principles
 GASSP, 183
 IT security standards, 183
- Importance of COSO internal controls, COSO internal controls framework, 66
- Incident management, ITIL service operation processes, 103
- Information and communication flows, ERM components, 150
- Information processing, control activities, 58
- Information Systems Audit and Control Association (ISACA), IT auditors, 323
- Information systems security, ITIL service strategy processes, 98
- Information Technology Infrastructure Library (ITIL)
 IT Service Management (ITSM), 87
 ITIL continuous feedback cycle, 89
 ITIL fundamentals, 88
- Infrastructure portfolios, IT portfolio management, 260
- Inherent risk, risk management fundamentals, 144
- Institute of Internal Auditors (IIA)
 Internal audit background, 321
 internal audit standards, IT governance standards, 329
 IT auditors, 323
- Integrity and ethical values, COSO control environment components, 55
- Internal audit background
 Institute of Internal Auditors (IIA), 321
 Internal audit responsibilities, 320
- Internal audit charters, internal audit processes, 325

- Internal audit processes
 - audit evidence classifications, 328
 - internal audit charters, 325
 - IT Governance Focus Areas, 330
 - performing internal audits, 327
 - planning and authorizing internal audits, 324
 - reporting internal audit results, 328
 - testing audit evidence, 327
- Internal audit responsibilities
 - audit committees, 373
 - internal audit background, 320
- Internal audit reviews
 - IT performance measurement processes, 333
 - IT resource management processes, 332
 - IT risk management processes, 332
 - IT value delivery processes, 331
- Internal audit roles, Section 404 internal controls assessments, 15
- Internal control deficiencies, internal control reporting processes, 62
- Internal control definition, COSO internal controls, 49
- Internal control evaluation processes
 - benchmarking, 62
 - COSO internal control framework, 62
 - COSO monitoring design and implementation process, 66
 - internal control monitoring processes, 65
- Internal control issues, IT service-oriented architecture (SOA), 235
- Internal control monitoring processes, internal control evaluation processes, 65
- Internal control planning considerations, Section 404 internal controls assessments, 16
- Internal control reporting processes
 - internal control deficiencies, 62
 - materiality considerations, 63
- Internal control standards background
 - COSO internal controls, 51
 - definition of internal control, 51
- Internal controls definition
 - COSO internal control framework, 53
 - IT internal controls, 50
- Internal Organization for Standards, (ISO), 110
- International Information Systems Security Certification Consortium (ISC)², IT security standards, 179
- ISACA, IT Governance Institute (ITGI), 68
- (ISC)², IT security standards, 179
- ISO 27002, ISO IT security standards, 115
- ISO 27002 implementation steps, IT security management processes, 117
- ISO 27002 standards topic areas, ISO IT security standards, 116
- ISO 38500 enterprise IT governance model, ISO standards, 121
- ISO 38500 implementation steps, IT governance guidance, 122
- ISO 38500 IT governance standards, ISO standards, 118
- ISO 38500 objectives, IT governance, 120
- ISO 38500 principles, COBIT, 119
- ISO 9000 quality management standards
 - ISO standards, 112
 - quality management system process, 114
- ISO certification process, ISO standards, 111
- ISO Documentation hierarchy, ISO standards, 114
- ISO IT security guidance, IT security model concepts, 185
- ISO IT security standards
 - ISO 27002, 115
 - ISO 27002 Standards Topic Areas, 116
- ISO standards
 - internal organization for standards, 110
 - ISO 38500 enterprise IT governance model, 121

- ISO standards (*continued*)
 - ISO 38500 IT governance standards, 118
 - ISO 9000 quality management standards, 112
 - ISO certification process, 111
 - ISO documentation hierarchy, 114
 - quality management standards, 112
- IT accounting, ITIL financial management, 94
- IT application controls, cloud computing application controls, 164
- IT application of management, IT portfolio management, 259
- IT applications, internal controls
 - ECM concepts, 310
 - storage management virtualization, 168
- IT applications, social media systems, 355
- IT architecture enablers
 - COBIT 5 simplified general architecture, 73
 - COBIT principles, 72
- IT architectures
 - IT service-oriented architecture (SOA), 232
 - service-driven IT applications, 232
- IT audit guidance, COSO internal controls framework, 68
- IT audit review activities, IT governance, 333
- IT auditors
 - Information Systems Audit and Control Association (ISACA), 323
 - Institute of Internal Auditors (IIA), 323
- IT budgeting, ITIL financial management, 93
- IT capacity management, IT configuration management
 - concepts, 250
- IT cloud computing concepts, cloud computing descriptions, 162
- IT configuration management, ITIL best practices, 251
- IT configuration management concepts
 - configuration management definition, 249
 - IT capacity management, 250
 - IT governance issues, 250
 - IT problem management, 250
 - service level agreements (SLAs), 250
- IT configuration management systems
 - configuration management database (CMDB), 247
 - IT governance, 247
 - IT infrastructure components, 248
 - ITIL best practices, 248
- IT continuity planning
 - disaster recovery planning, 187
 - IT governance, 186
- IT customer needs, IT service catalogs, 220
- IT general controls, ITIL strategic capabilities, 92
- IT governance
 - audit committee internal control issues, 375
 - board of directors and audit committee, 371
 - Business Continuity Plan (BCP) Life Cycle, 190
 - business continuity planning, 188
 - change management processes, 100
 - configuration management processes, 102
 - ECM Architecture, 313
 - ECM processes, 310
 - enterprise codes of conduct, 341
 - enterprise content management (ECM), 309
 - enterprise ethics hotline functions, 350
 - enterprise governance issues, 28
 - ethical workplace cultures, 337
 - financial management of IT systems, 95
 - governance, risk, and compliance processes, 45
 - impact of social media computing, 365

- implementing IT configuration management, 253
- internal audit processes, 324
- ISO 38500 Objectives, 120
- IT audit review activities, 333
- IT configuration management systems, 247
- IT continuity planning, 186
- IT portfolio management, 259
- IT service catalog business relationships, 222
- IT service functions, 233
- IT service level agreements (SLAs), 287
- IT service-oriented architecture (SOA), 242
- IT systems development processes, 264
- IT systems security objectives, 99
- IT value management initiatives, 300
- IT virtualization, 170
- ITIL service delivery best practices, 106
- mission statements, 337
- OCEG model, 297
- Open Compliance and Ethics Group (OCEG), 153, 292
- Payment Card Industry Data Security Standard (PCI DSS), 195
- program management office (PMO), 284
- project, program, and portfolio management overview, 286
- RAD Controls and Procedures, 269
- SLAs, 287
- social media applications, 370
- tangible and intangible ERP system benefits, 272
- Val IT, 298
- Val IT framework, 299
- IT governance risk issues, IT governance concepts, 30
- IT governance and management, COBIT principles, 80
- IT governance cloud computing concerns
 - cloud computing data location issues, 167
 - cloud computing investigative support, 167
 - cloud computing long-term viability issues, 167
 - cloud computing recovery issues, 167
 - cloud computing regulatory compliance, 167
 - privileged user access issues, 167
- IT governance concepts
 - business performance, 6
 - corporate ethics, 9
 - COSO enterprise risk management (ERM) framework, 30
 - definition of IT governance, 29
 - enterprise IT governance goals, 7
 - enterprise organization issues, 32
 - GRC governance elements, 41
 - GRC principles, 38
 - IT governance risk issues, 30, 31
 - IT governance enterprise issues, 33
 - IT governance security issues, 34
 - IT security controls, 34
 - jurisdiction and boundary issues, 32
 - legislative and regulatory issues, 32
 - measures of IT governance success, 6
 - risk appetite, 31
 - risk management concerns, 40
 - Sarbanes-Oxley Act (SOx) rules, 5
- IT governance controls, IT service-oriented architecture (SOA), 245
- IT governance elements
 - GRC concepts, 39
 - Sarbanes-Oxley Act (SOx), 10
- IT governance enterprise issues, IT governance concepts, 33
- IT governance focus, COBIT strengths, 85
- IT governance focus areas, internal audit processes, 330
- IT governance guidance
 - COSO internal controls framework, 68
 - ISO 38500 implementation steps, 122
- IT Governance Institute, Val IT, 298
- IT Governance Institute (ITGI)
 - COBIT, 68
 - ISACA, 68

- IT governance issues
 - Enron failure, 9
 - IT configuration management
 - concepts, 250
 - IT service-oriented architecture (SOA), 235
 - risk management fundamentals, 126
 - security issues, 34
 - smartphone and handheld devices, 175
 - SOA implementation blueprint, 241
 - SOA policies and procedures, 238
- IT governance objectives
 - COSO internal controls, 49
 - definition of IT governance, 30
 - OCEG GRC capability model, 154
- IT governance policies, smartphone and handheld devices, 176
- IT governance principles, COBIT, 70
- IT governance requirements, HIPAA, 212
- IT governance responsibilities, audit committees, 374
- IT governance risk issues
 - IT governance concepts, 31
 - IT password standards, 31
 - risk appetite, 31
- IT governance risks, social media systems, 355
- IT governance rules, Gramm-Leach-Bliley Act (GLBA), 205
- IT governance security issues, IT governance concepts, 34
- IT governance standards, Institute of Internal Auditors (IIA) internal audit standards, 329
- IT governance value objectives, COBIT principles, 75
- IT governance virtualization good practices, 174
- IT infrastructure
 - service delivery best practices, 88
 - service support processes, 89
- IT infrastructure components, IT configuration management systems, 248
- IT internal controls, definition, 50
- IT management concerns, IT security, 178
- IT objectives, IT-related COBIT goals, 83
- IT operations, IT service level agreements (SLAs), 291
- IT password standards, IT governance risk issues, 31
- IT performance measurement processes, internal audit reviews, 333
- IT portfolio management
 - application portfolios, 260
 - infrastructure portfolios, 260
 - IT application of management, 259
 - IT governance, 259
 - project portfolios, 261
 - project, program, and portfolio management overview, 283
- IT privacy legislation, Gramm-Leach-Bliley Act (GLBA), 203
- IT privacy rules
 - Health Insurance Portability and Accountability Act (HIPAA), 208
 - HIPAA patient record privacy rules, 209
- IT problem management, IT configuration management concepts, 250
- IT program management
 - project, program, and portfolio management overview, 283
- IT project management
 - project, program, and portfolio management overview, 283
- IT resource management processes, internal audit reviews, 332
- IT risk management enablers, COBIT principles, 78
- IT risk management processes, internal audit reviews, 332
- IT security
 - costs and benefits, 180
 - IT management concerns, 178
 - management practices, 180
 - societal factors constraints, 182

- systems owners security responsibilities, 181
- IT security administrative procedures, HIPAA, 213
- IT security controls, IT governance concepts, 34
- IT security management processes, ISO 27002 implementation steps, 117
- IT security model concepts
 - COBIT IT security guidance, 185
 - ISO IT security guidance, 185
- IT security practices, business continuity planning, 192
- IT security processes, ECM security tools, 313
- IT security purposes, GASSP principles, 179
- IT security standards
 - (ISC)², 179
 - GASSP body of knowledge, 184
 - generally accepted system security principles (GASSP), 179
 - GLBA, 203
 - Gramm-Leach-Bliley Act (GLBA), 203
 - implementing IT security principles, 183
 - International Information Systems Security Certification Consortium (ISC)², 179
 - Payment Card Industry Data Security Standard (PCI DSS), 195
- IT service catalog business relationships, IT governance, 222
- IT service catalogs
 - IT customer needs, 220
 - IT system of record, 221
 - service catalog characteristics, 218
 - service request processes, 220
- IT service functions, IT governance, 233
- IT service level agreement (SLA) contents, 290
- IT service level agreements (SLAs)
 - IT governance, 287
 - IT operations, 291
 - IT service level agreement contents, 290
- IT Service Management Forum (itSMF), 287
- Information Technology Infrastructure Library (ITIL), 87
- IT Service Management Forum (itSMF)
 - best practices standards for IT service support, 288
 - IT service level agreements (SLAs), 287
 - ITIL, 288
- IT service-oriented architecture (SOA)
 - design-time policies, 240
 - internal control issues, 235
 - IT architectures, 232
 - IT governance controls, 245
 - IT governance issues, 235
 - SOA characteristics, 232
 - web services applications, 243
- IT system of record, IT service catalogs, 221
- IT system risks, impact of social media computing, 365
- IT systems development efforts, project management, 275
- IT systems development processes, IT governance, 264
- IT systems internal controls, IT virtualization, 173
- IT systems security objectives, IT governance, 99
- IT systems virtualization, definition, 162
- IT value delivery processes, internal audit reviews, 331
- IT value management initiatives, IT governance, 300
- IT value management readiness
 - assessment, Val IT, 301
- IT virtualization
 - IT governance, 170
 - IT governance virtualization good practices, 174
 - IT systems internal controls, 173
 - virtualization definitions, 169

ITIL

- IT Service Management Forum (itSMF), 288
 - service delivery best practices, 88
 - service feedback processes, 90
 - service support processes, 89
 - ITIL best practices, IT configuration management, 251
 - ITIL change management, ITIL service strategy processes, 100
 - ITIL continuous feedback cycle, Information Technology Infrastructure Library (ITIL), 89
 - ITIL financial management
 - charging for IT services, 94
 - IT accounting, 94
 - IT budgeting, 93
 - ITIL service strategy components, 93
 - ITIL fundamentals
 - Information Technology Infrastructure Library (ITIL), 88
 - ITIL service operation processes, 103
 - service strategy components, 91
 - ITIL incident management life cycle,
 - service operation event and incident management, 104
 - ITIL service delivery best practices, IT governance, 106
 - ITIL service operation processes
 - incident management, 103
 - ITIL fundamentals, 103
 - problem management, 105
 - service operation event and incident management, 103
 - service operation problem management, 105
 - ITIL service strategy components
 - financial management for IT services, 93
 - ITIL financial management, 93
 - ITIL service strategy processes
 - availability management, 96
 - capacity management, 95
 - continuity management, 98
 - information systems security, 98
 - ITIL change management, 100
 - service delivery availability management, 96
 - service delivery capacity management, 95
 - service delivery continuity management, 98
 - service delivery information systems security, 98
 - service transition change management, 100
 - ITIL strategic capabilities, IT general controls, 92
 - ITIL transition management processes
 - configuration management, 101
 - service transition configuration management, 101
 - IT-oriented internal control assessments, COBIT, 57
 - IT-related COBIT goals
 - IT objectives, 83
 - mapping COBIT processes, 82
 - IT-related internal controls, COSO internal controls, 50
- J**
- Johnson & Johnson Tylenol crisis, mission statements, 338
 - Jurisdiction and boundary issues, IT governance concepts, 32
- L**
- Legislative and regulatory issues, IT governance concepts, 32
- LinkedIn
- market research application, 360
 - social media system examples, 360
- M**
- Management of enterprise IT, COBIT processes, 81
 - Management philosophy and operational style, COSO control environment components, 55
 - Management practices, IT security, 180

- Mapping COBIT processes, IT-related
 - COBIT goals, 82
 - Mapping IT governance relationships, COSO Components and COBIT Objectives, 85
 - Market research application, LinkedIn, 360
 - Materiality considerations, internal control reporting processes, 63
 - Measures of IT governance success, IT governance concepts, 6
 - Medical records disclosures, HIPAA
 - patient record privacy rules, 210
 - Mission statements
 - IT governance, 337
 - Johnson & Johnson Tylenol crisis, 338
 - Mitigation strategies, risk identification, 41
 - Monitoring, COSO Internal Control Framework, 60
 - Monitoring and auditing, GLBA
 - safeguards compliance, 206
 - Monitoring guidance, COSO internal control framework, 65
- N**
- National Commission on Fraudulent Financial Reporting
 - COSO, 52
 - Treadway Commission, 52
- O**
- OCEG GRC capability model
 - GRC subpractices, 159
 - IT governance objectives, 154
 - Principled Performance, 154
 - OCEG model, IT governance, 297
 - OCEG Red Book
 - GRC capability model, 292
 - Open Compliance and Ethics Group (OCEG), 153
 - Officer disclosure sign-off, CEO financial report certification, 24
 - Open Compliance and Ethics Group (OCEG)
 - GRC capability model elements, 293
 - GRC guidance, 292
 - IT governance, 153, 292
 - OCEG Red Book, 153
 - Principled Performance concept, 292
 - risk management, 153
 - Operations internal controls, COSO
 - internal control framework, 53
 - Organizational structure, COSO control environment components, 56
- P**
- Payment Card Industry (PCI) Data Security Standards Council, 196
 - Payment Card Industry Data Security Standard (PCI DSS)
 - IT governance, 195
 - IT security standards, 195
 - Payment Card Industry (PCI) Council, 196
 - self-assessment processes, 202
 - Payment card requirements, PCI DSS, 197
 - PCAOB (Public Company Accounting Oversight Board), Sarbanes-Oxley Act (SOx), 10
 - PCI DSS (Payment Card Industry Data Security Standard)
 - IT governance, 195
 - IT security standards, 195
 - Payment Card Industry (PCI) Council, 196
 - self-assessment processes, 202
 - Performance indicators, control Activities, 58
 - Performing internal audits, internal audit processes, 327
 - Physical controls, control activities, 58
 - Planning and authorizing internal audits, internal audit processes, 324
 - PMBOK. *See* Project Management Book of Knowledge (PMBOK)
 - Pretexting
 - GLBA pretexting rules, 206
 - Gramm-Leach-Bliley Act (GLBA), 203

- PRINCE2, project management standards, 280
 - PRINCE2 project management process, project management standards, 282
 - Principled Performance, OCEG GRC capability model, 154
 - Principled Performance concept, Open Compliance and Ethics Group (OCEG), 292
 - Privileged user access issues, IT governance cloud computing concerns, 167
 - Pro forma financial reports, Sarbanes-Oxley Act (SOx), 25
 - Problem management
 - ITIL service operation processes, 105
 - request for change (RFC) documents, 105
 - Process flowcharting, COSO ERM monitoring, 152
 - Program management office (PMO), IT governance, 284
 - Project definition, *Project Management Book of Knowledge* (PMBOK), 277
 - Project management, IT systems development efforts, 275
 - Project Management Book of Knowledge* (PMBOK)
 - process groups and knowledge areas, 279
 - project definition, 277
 - Project Management Institute (PMI), 276
 - project management process, 278
 - project management standards, 276
 - Project Management Institute (PMI), *Project Management Book of Knowledge* (PMBOK), 276
 - Project management standards
 - PRINCE2, 280
 - PRINCE2 Project Management Process, 282
 - Project Management Book of Knowledge (PMBOK), 276
 - Project portfolios, IT portfolio management, 261
 - Project, program, and portfolio management overview
 - IT governance, 286
 - IT portfolio management, 283
 - Public Company Accounting Oversight Board (PCAOB), Sarbanes-Oxley Act (SOx), 10
- Q**
- Qualitative risk assessments, risk management fundamentals, 128
 - Quality management standards
 - ISO standards, Deming, Edward, 112
 - Quality management system process, ISO 9000 quality management standards, 114
 - Quantitative risk assessments, risk management fundamentals, 128
- R**
- RAD controls and procedures, IT governance, 269
 - Rapid application development (RAD) application systems development, 267
 - client–server systems applications development, 268
 - Reporting internal audit results, internal audit processes, 328
 - Request for change (RFC) documents, problem management, 105
 - Requirements analysis process, systems development life-cycle (SDLC) phases, 266
 - Residual risk, risk management fundamentals, 144
 - Risk acceptance, risk management strategies, 146
 - Risk appetite
 - COSO ERM framework, 135
 - IT governance concepts, 31
 - IT governance risk issues, 31

- Risk appetite map, COSO ERM framework, 139
 - Risk assessment, COSO internal control framework, 57
 - Risk assessment analysis
 - risk likelihood, 129
 - risk significance, 129
 - Risk avoidance, risk management strategies, 145
 - Risk event–risk response activities, COSO ERM risk event–risk response activities, 147
 - Risk identification
 - mitigation strategies, 41
 - risk management fundamentals, 127
 - Risk impact, risk management fundamentals, 145
 - Risk likelihood
 - risk assessment analysis, 129
 - risk management fundamentals, 145
 - Risk Management, Open Compliance and Ethics Group (OCEG), 153
 - Risk management concerns
 - IT governance concepts, 40
 - risk monitoring, 42
 - Risk management fundamentals
 - enterprise business risks, 129
 - inherent risk, 144
 - IT governance issues, 125
 - qualitative risk assessments, 128
 - quantitative risk assessments, 128
 - residual risk, 144
 - risk identification, 127
 - risk impact, 145
 - risk likelihood, 145
 - risk monitoring, 133
 - risk portfolio management, 147
 - risk response planning, 131
 - Risk management overview, GRC compliance, 42
 - Risk management philosophy, COSO ERM framework, 138
 - Risk management strategies
 - risk acceptance, 146
 - risk avoidance, 145
 - risk reduction, 145
 - Risk monitoring
 - risk management concerns, 42
 - risk management fundamentals, 133
 - Risk monitoring activities, COSO ERM monitoring, 151
 - Risk portfolio management, risk management fundamentals, 147
 - Risk reduction, risk management strategies, 145
 - Risk response planning, risk management fundamentals, 131
 - Risk significance, risk assessment analysis, 129
 - Risk-based approaches, AS5, 27
 - Runtime policies and processes, SOA governance, 241
- S**
- Sarbanes-Oxley Act (SOx)
 - audit committee financial expert rules, 23
 - auditor independence, 18
 - CEO financial report certification, 23
 - conflict-of-interest provisions, 26
 - corporate responsibilities, 22
 - external audit partner rotation, 21
 - external audit process rules, 12
 - IT governance elements, 10
 - pro forma financial reports, 25
 - Public Company Accounting Oversight Board (PCAOB), 10
 - Section 404 internal controls assessments, 14
 - SOx key provisions summary, 11
 - SOx officer disclosure sign-off, 25
 - whistleblower rules, 23
 - Sarbanes-Oxley Act (SOx) rules, IT governance concepts, 5
 - SAS No. 1, definition of internal control, 51
 - SAS 70, cloud computing application controls, 164
 - SDLC life cycle, systems development life-cycle (SDLC) phases, 265

- SDLC processes
 - design-time SOA processes, 240
 - SOA life cycle, 240
- Section 404 internal controls
 - assessments
 - AS5 rules, 17
 - basic accounting cycles, 15
 - external auditor service limitations, 19
 - internal audit roles, 15
 - internal control planning
 - considerations, 16
 - Sarbanes-Oxley Act (SOx), 14
- Security and data protection controls,
 - CMDB components, 255
- Security and privacy challenges, cloud
 - computing concepts, 166
- Security issues, IT governance issues, 34
- Security services and mechanisms,
 - HIPAA security requirements, 214
- Segregation of duties, control activities, 58
- Self-assessment processes, payment card
 - industry data security standard, 202
- Senior financial officer SOx requirements,
 - codes of ethics, 26
- Service catalog
 - characteristics, 223
 - elements, 223
 - IT service catalogs, 218
 - management, 224
- Service delivery availability management,
 - ITIL service strategy processes, 96
- Service delivery best practices
 - IT infrastructure, 88
 - ITIL, 88
- Service delivery capacity management,
 - ITIL service strategy processes, 95
- Service delivery continuity management,
 - ITIL service strategy processes, 98
- Service delivery information systems
 - security, ITIL service strategy processes, 98
- Service-driven IT applications, IT
 - architectures, 232
- Service feedback processes, ITIL, 90
- Service level agreements (SLAs), SOA
 - governance, 241
- Service level agreements (SLAs),
 - IT configuration management concepts, 250
- Service operation event and incident
 - management
 - ITIL incident management life cycle, 104
 - ITIL service operation processes, 103
- Service operation problem management,
 - ITIL service operation processes, 105
- Service-oriented architecture. *See* SOA
 - characteristics
- Service request processes, IT service
 - catalogs, 220
- Service strategy components, ITIL
 - fundamentals, 91
- Service support processes
 - IT infrastructure, 89
 - ITIL, 89
- Service transition change management,
 - ITIL service strategy processes, 100
- Service transition configuration
 - management, ITIL transition management processes, 101
- SLAs, IT governance, 287
- Smartphone and handheld devices
 - IT governance issues, 175
 - IT governance policies, 176
- SOA characteristics
 - enterprise IT general controls, 233
 - IT service-oriented architecture (SOA), 232
 - SOA enterprise configurations, 234
 - SOA service aggregation, 233
- SOA enterprise configurations, SOA
 - characteristics, 234
- SOA governance
 - runtime policies and processes, 241
 - service level agreements, 241
 - stakeholder SOA life-cycle roles and responsibilities, 239

- SOA implementation blueprint, IT
 - governance issues, 241
 - SOA life cycle, SDLC processes, 240
 - SOA policies and procedures, IT
 - governance issues, 238
 - SOA service aggregation, SOA
 - characteristics, 233
 - Social media applications, IT governance, 370
 - Social media IT applications history,
 - social media systems, 356
 - Social media policy, social media systems, 368
 - Social media system examples
 - Facebook, 358
 - LinkedIn, 360
 - Twitter, 362
 - Social media systems
 - impact of social media computing, 364
 - IT applications, 355
 - IT governance risks, 355
 - social media IT applications history, 356
 - social media policy, 368
 - Societal factors constraints, IT security, 182
 - SOx compliance processes, ethical standards, 27
 - SOx internal controls requirements, COBIT, 71, 84
 - SOx key provisions summary, Sarbanes-Oxley Act (SOx), 11
 - SOx officer disclosure sign-off, Sarbanes-Oxley Act (SOx), 25
 - SOx rules, audit committees, 372
 - SOx Section 404, COBIT, 84
 - Stakeholder SOA life-cycle roles and responsibilities, SOA governance, 239
 - Storage management virtualization, IT
 - applications internal controls, 168
 - Systems development life-cycle (SDLC)
 - phases
 - requirements analysis process, 266
 - SDLC life cycle, 265
 - Systems development life-cycle (SDLC)
 - processes, application systems development, 264
 - Systems owners security responsibilities,
 - IT security, 181
- T**
- Tangible and intangible ERP system
 - benefits
 - enterprise resource planning (ERP) systems, 272
 - IT governance, 272
 - Testing audit evidence, internal audit
 - processes, 327
 - Tone at the top, COSO control
 - environment, 54
 - Top-level reviews, control activities, 58
 - Treadway Commission
 - COSO internal controls framework, 52
 - National Commission on Fraudulent Financial Reporting, 52
 - Twitter, terms and concepts, 363
- U**
- U.S. National Research Council,
 - Computers at Risk (CAR), 179
- V**
- Val IT
 - IT governance, 298
 - IT Governance Institute, 298
 - IT value management readiness assessment, 301
 - Val IT best practices governance
 - framework, COBIT, 298
 - Val IT framework, IT governance, 299
 - Virtualization definitions, 162, 169
- W**
- Web services applications, IT service-oriented architecture (SOA), 243
 - Whistleblower and hotline functions
 - enterprise codes of conduct, 346
 - Federal whistleblower rules, 348
 - Whistleblower rules, Sarbanes-Oxley Act (SOx), 23

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>