

Index

- A**
- Access management provisioning processes
 - processes for managing access to enterprise IT resources, 478
 - ACL CAATT example
 - developing and processing CAATTs, 319
 - ACL continuous assurance systems
 - computer-assisted audit tools and techniques (CAATT), 337
 - Acquisition and implementation control objectives
 - CobiT to assess internal controls, 43
 - American Society for Quality (ASQ)
 - ASQ internal auditor certifications, 629
 - certified quality auditors (CQA), 630
 - quality audit division (QAD), 633
 - Application control elements
 - application input components, 231
 - application output components, 239
 - computer program architectures, 235
 - IT audit procedures, 230
 - Application control objectives
 - application controls reviews, 247
 - Application controls reviews
 - application control objectives, 247
 - application input and output IT audit tests, 257
 - application process block diagrams, 245
 - application review walk-through, 244
 - applications under development, 258
 - application testing and implementation objectives, 264
 - automated purchasing system compliance tests example, 253
 - computer-assisted audit tools and techniques (CAATTs), 253
 - IT application review audit procedures, 249
 - IT application review processing controls, 251
 - IT audit procedures, 242
 - performing an application walkthrough, 245
 - post implementation review objectives, 264
 - testing audit control objectives, 249
 - tests of application inputs and outputs, 252
 - web services applications, 295
 - Application development review guidelines
 - IT audit procedures, 237
 - Application input and output it audit tests
 - application controls reviews, 257
 - Application input components
 - application control elements, 231
 - Application output components
 - application control elements, 239
 - Application process block diagrams
 - application controls reviews, 245
 - Application review walk-through
 - application controls reviews, 244
 - Application selection risk factors
 - IT application controls, 240
 - Applications review IT audit plan
 - performing effective IT audits, 125
 - Applications under development
 - application controls reviews, 258
 - preimplementation review problems, 261
 - preimplementation review procedures, 262
 - Application testing and implementation objectives
 - application controls reviews, 264
 - Application tests of compliance
 - IT audit procedures, 257
 - AS5 objectives
 - section 404 internal controls review, 29
 - ASQ internal auditor certifications
 - American Society for Quality (ASQ), 629
 - Assessing enterprise management controls
 - audit professional responsibilities, 3
 - Assignment of authority and responsibility
 - COSO internal control framework, 12
 - Association for Information and Image Management
 - electronic documentation standards, 516
 - Association of Certified Fraud Examiners (ACFE)
 - certified fraud examiner (CFE), 625
 - fraud detection and prevention, 454
 - Attributes sampling advantages and limitations
 - attributes sampling tests, 142
 - Attributes sampling tests
 - attributes sampling advantages and limitations, 142
 - audit sampling approaches, 137, 138
 - evaluating attributes sampling test results, 141

- Audit committee
 - chief audit executive (CAE), 355
 - Audit committee reports
 - IT audit significant findings, 361
 - Audit committee reviews
 - IT audit significant findings, 360
 - Audit evidence
 - IT auditor “best evidence” classification, 133
 - performing effective IT audits, 132
 - Audit evidence gathering
 - computer-assisted audit tools and techniques (CAATT), 327
 - Audit guidelines for developing a CAATT
 - computer-assisted audit tools and techniques (CAATT), 312
 - Auditing a disaster recovery plan (DRP)
 - internal audit disaster recovery plan reviews, 491
 - IT audit procedures, 489
 - Auditing BCM processes
 - IT audit procedures, 540
 - Auditing change and patch management procedures
 - IT audit procedures, 573
 - Auditing COSO ERM
 - IT audit procedures, 114
 - Auditing electronic document management processes
 - IT audit procedures, 520
 - Auditing enterprise BCM processes
 - IT audit procedures, 541
 - Auditing Gramm-Leach-Bliley Act compliance
 - IT audit procedures, 395
 - Auditing HIPAA requirements procedures
 - IT audit procedures, 399
 - Auditing identity and access management processes
 - IT audit procedures, 484
 - Auditing service-oriented architectures
 - IT audit procedures, 296
 - Auditing SOA environments
 - IT audit procedures, 294
 - Auditing SOA governance general controls
 - IT audit procedures, 296
 - Auditing standards
 - SAS No. 1, 7
 - Auditing user-initiated transactions
 - computer-assisted audit tools and techniques (CAATT), 320
 - Auditing web services applications
 - IT audit procedures, 298
 - Audit planning memo
 - performing effective IT audits, 124
 - Audit procedures files
 - workpaper documentation, 147
 - Audit professional responsibilities
 - assessing enterprise management controls, 3
 - COSO internal controls framework, 3
 - COSO internal control standards, 4
 - Audit program preparation procedures
 - organizing IT audit functions, 601
 - Audit programs
 - performing effective IT audits, 125
 - Audit sampling approaches
 - attributes sampling tests, 137, 138
 - discovery sampling, 137
 - performing effective IT audits, 133
 - variables sampling, 136
 - Audit sampling benefits
 - performing effective IT audits, 135
 - Audit test and analysis software
 - computer-assisted audit tools and techniques (CAATT), 322
 - Authentication and authorization processes
 - IT security controls, 479
 - Automated identity and access management processes
 - IT audit procedures, 475
 - Automated purchasing system compliance tests example
 - application controls reviews, 253
- B**
- Basic knowledge requirements
 - IT audit specialists, 597
 - BCM incident timelines
 - business continuity management, 536
 - BCM response strategies
 - business continuity development processes, 535
 - BCM test exercise types
 - business continuity management, 539
 - Benchmarking
 - Internal control evaluation process, 18
 - Benefits of IT audit quality-assurance reviews
 - IT audit function quality assurance reviews, 642
 - Bhopal gas leak
 - enterprise risks, 91
 - Black belt body of knowledge
 - six sigma, 583
 - Board of Directors and Audit Committee.
 - COSO internal control framework, 11
 - BS 25999 good practice guidelines
 - ISO 27002, 543
 - Building a DRP
 - DRP deliverables, 498
 - fully mirrored recovery operations, 500
 - hot site facilities, 500
 - IT disaster recovery planning processes, 497
 - Business continuity and disaster recovery strategies
 - ITIL continuity management, 189

- Business continuity development processes
 - BCM response strategies, 535
 - business continuity management, 526
 - developing effective BCM strategies, 533
 - incident management plans, 535
 - incident response structures, 535
 - Business continuity management
 - BCM incident timelines, 536
 - BCM test exercise types, 539
 - business continuity development processes, 526
 - business continuity management life cycle, 525
 - business continuity planning processes, 521
 - business impact analysis drivers, 527
 - continuity management strategies, 532
 - risk assessments, 530
 - testing BCM plans, 538
 - Business continuity management life cycle
 - business continuity management, 525
 - Business continuity planning processes
 - business continuity management, 521
 - Business continuity plan requirements
 - IT audit procedures, 537
 - Business continuity plan training
 - IT disaster recovery planning processes, 503
 - Business continuity processes
 - business impact analysis, 522
 - Business criticality risk analysis schedule
 - business impact analysis, 499
 - Business impact analysis
 - business continuity processes, 522
 - business criticality risk analysis schedule, 499
 - DRP client-server readiness reviews, 498
 - impact analysis criteria, 528
 - risk assessment process steps, 531
 - Business impact analysis drivers
 - business continuity management, 527
 - Business requirements
 - CobiT cube components, 39
 - Business unit entity-level risks
 - entity-level risks, 113
- C**
- CAA/CM processes
 - computer-assisted audit tools and techniques (CAATT), 333
 - continuous assurance auditing conceptual model, 334
 - CAA resource requirements
 - Continuous assurance auditing (CAA), 335
 - CAATT objectives
 - IT audit procedures, 307
 - CAATT software tools
 - continuous audit monitor CAATT, 325
 - developing and processing CAATTs, 311
 - report generators languages, 316
 - CAE responsibilities
 - internal audit functions, 595
 - Capability maturity model for integration (CMMi)
 - monitoring and evaluation (ME) control objectives, 51
 - Capacity management sub processes
 - ITIL capacity management, 186
 - Categories of IT application changes and patches
 - IT application change management processes, 565
 - CCSA examination
 - CCSA examination topics, 625
 - CCSA examination and requirements
 - certification in control self-assessment (CCSA), 623
 - CCSA examination topics
 - CCSA examination, 625
 - Certificate in the governance of enterprise IT (CGEIT)
 - CGEIT examination content areas, 612
 - CGEIT requirements, 611
 - Certification in control self-assessment (CCSA)
 - CCSA examination and requirements, 623
 - Certified fraud examiner (CFE)
 - Association of Certified Fraud Examiners (ACFE), 625
 - Certified information security manager (CISM)
 - CISM examination content areas, 610
 - CISM requirements, 609
 - Certified information systems auditor (CISA)
 - CISA examination content areas, 608
 - CISA requirements, 608
 - professional certifications, 607
 - Certified information system security professional (CISSP)
 - CISSP requirements, 628
 - international information systems security certification consortium, 628
 - Certified internal auditor (CIA)
 - CIA requirements, 612
 - Certified internal auditor responsibilities and requirements
 - CIA examination summary, 614
 - Certified quality auditors (CQA)
 - American Society for Quality (ASQ), 630
 - CQA examination and requirements, 630
 - quality auditor responsibilities, 633
 - quality audit types, 636
 - CFAA provisions
 - Computer Fraud and Abuse Act (CFAA), 387
 - CFSA examination and requirements
 - CFSA insurance industry examination topics, 628
 - CFSA insurance industry examination topics
 - CFSA examination and requirements, 628

- CGEIT examination content areas
 - certificate in the governance of enterprise IT (CGEIT), 612
- CGEIT requirements
 - certificate in the governance of enterprise IT (CGEIT), 611
- Change and patch management control processes
 - IT internal control procedures, 558
- Change management metric measures
 - IT application change management processes, 568
- Checklist format audit programs, 131
- performing effective IT audits, 129
- Chief audit executive (CAE)
 - audit committee, 355
- CIA
 - CIA requirements, 612
- CIA examination
 - CIA examination summary, 613
 - maintaining CIA certifications, 623
- CIA examination summary
 - certified internal auditor responsibilities and requirements, 614
 - CIA examination, 613
- CIA requirements
 - certified internal auditor (CIA), 612
- CISA examination content areas
 - certified information systems auditor (CISA), 608
- CISA requirements
 - certified information systems auditor (CISA), 608
- CISM examination content areas
 - certified information security manager (CISM), 610
- CISM requirements
 - certified information security manager (CISM), 609
- CISSP requirements
 - certified information system security professional (CISSP), 628
- Client-server and smaller-systems general IT controls
 - IT general controls, 165
- Client-server IT process continuity planning
 - IT emergency response procedures, 495
- Cloud computing application controls
 - IT audit procedures, 222
- Cloud computing concepts
 - cloud computing security and privacy, 223
 - evolving control issues, 220
 - IT operating system fundamentals, 220
 - software as a service (SaaS), 221
- Cloud computing security and privacy
 - cloud computing concepts, 223
- Cloud computing service provider selection
 - IT audit procedures, 224
- CMMi
 - CMMi key process areas (KPA), 274
 - KPA status review IT audit procedures, 275
 - software engineering concepts, 267
 - software engineering institute capability maturity model, 267
- CMMi IT audit processes
 - IT audit procedures, 281
- CMMi key process areas (KPA)
 - CMMi, 274
- CMMi level 1
 - CMMi maturity levels, 271
 - systems development activities, 272
- CMMi level 2
 - CMMi level 2 KPA requirements, 274
 - CMMi maturity levels, 273
- CMMi level 3
 - CMMi level 3 KPA requirements, 278
 - CMMi maturity levels, 277
- CMMi level 4
 - CMMi level 4 activities, 279
 - CMMi maturity levels, 279
- CMMi level 5
 - CMMi maturity levels, 280
- CMMi level 4 activities
 - CMMi level 4, 279
- CMMi level 2 KPA requirements
 - CMMi level 2, 274
- CMMi level 3 KPA requirements
 - CMMi level 3, 278
- CMMi level 1 to level 2 differences
 - CMMi maturity levels, 273
- CMMi maturity levels
 - CMMi level 1, 271
 - CMMi level 2, 273
 - CMMi level 3, 277
 - CMMi level 4, 279
 - CMMi level 5, 280
 - CMMi level 1 to level 2 differences, 273
 - software engineering concepts, 270
- CobiT
 - ISACA standards, 32
- CobiT cube
 - CobiT internal controls framework, 37
- CobiT cube components
 - business requirements, 39
 - IT resources, 37, 38
- CobiT framework
 - CobiT governance focus areas, 33
 - CobiT internal control concerns, 35
 - COSO internal controls framework, 36
 - Val IT guidance materials, 365
- CobiT governance focus areas
 - CobiT framework, 33
- CobiT internal control concerns
 - CobiT framework, 35
- CobiT internal controls framework
 - CobiT cube, 37

- CobiT objectives
 - COSO internal control framework, 52
- CobiT references
 - ITIL service management best practices, 177
- CobiT to assess internal controls
 - acquisition and implementation control objectives, 43
 - COSO internal controls, 40
 - delivery and support control objectives, 45
 - ITGI navigation framework, 40
 - monitoring and evaluation (ME) control objectives, 48
 - navigating the CobiT framework, 41
 - planning and organizing (PO) control objectives, 41
 - RACI charts, 42
 - section 404 internal controls reviews, 51
- Codes of conduct
 - integrity and ethical values, 10
 - IT auditor responsibility, 10
- Commitment to competence
 - COSO internal control framework, 11
- Communications and information
 - COSO internal control framework, 15
- Components of a DRP
 - IT audit procedures, 489
- Computer-assisted audit techniques
 - developing and processing CAATTs, 309
- Computer-assisted audit tools and techniques (CAATTs)
 - ACL continuous assurance systems, 337
 - application controls reviews, 253
 - audit evidence gathering, 327
 - audit guidelines for developing a CAATT, 312
 - auditing user-initiated transactions, 320
 - audit test and analysis software, 322
 - CAA/CM processes, 333
 - continuous assurance auditing (CAA), 329
 - continuous audit monitors, 324
 - continuous monitoring (CM), 332
 - generalized audit software, 311
 - IT audit procedures, 305
 - test data CAATT approach, 322
 - test deck approaches, 320
- Computer Fraud and Abuse Act (CFAA)
 - CFAA provisions, 387
 - IT-related laws, 386
- Computer program architectures
 - application control elements, 235
 - object-oriented programming language concepts, 236
- Computer Security Act of 1987
 - IT-related laws, 388
 - national institute of science and technology (NIST), 388
- Configuration management
 - configuration management database (CMDB), 192
 - ITIL service management best practices, 191
- Configuration management database (CMDB)
 - configuration management, 192
- Continuity management strategies
 - business continuity management, 532
- Continuity requirements analysis
 - estimating continuity requirements, 529
- Continuous assurance auditing
 - IT audit procedures, 339
- Continuous assurance auditing (CAA)
 - CAA resource requirements, 335
 - computer-assisted audit tools and techniques (CAATT), 329
 - dashboard monitoring approaches, 337
- Continuous assurance auditing conceptual model
 - CAA/CM processes, 334
- Continuous audit monitor CAATT
 - CAATT software tools, 325
- Continuous audit monitor example
 - developing and processing CAATTs, 332
- Continuous audit monitors
 - computer-assisted audit tools and techniques (CAATT), 324
- Continuous monitoring (CM)
 - computer-assisted audit tools and techniques (CAATT), 332
- Control activities
 - COSO ERM framework, 107
 - COSO internal control framework, 14
- Control and security characteristics
 - IT wireless networks, 216
- Control environment
 - COSO internal control framework, 10
- COSO communications and information
 - COSO internal control framework, 15
- COSO control activities
 - COSO internal control framework, 14
- COSO ERM
 - IT audit task, 113
 - IT change management requirements, 562
 - risk management fundamentals, 83
- COSO ERM framework
 - control activities, 107
 - COSO internal controls, 97, 100
 - enterprise risk management definition, 97
 - entity-level risks, 112
 - event identification, 103
 - information and communication, 108
 - legal and regulatory compliance risk objectives, 110
 - risk appetite, 98
 - risk assessments, 104
 - risk management objectives, 109
 - risk response strategies, 105

- COSO internal control framework
 - assignment of authority and responsibility, 12
 - Board of Directors and Audit Committee., 11
 - CobiT objectives, 52
 - commitment to competence, 11
 - communications and Information, 15
 - control activities, 14
 - control environment, 10
 - COSO communications and information, 15
 - COSO control activities, 14
 - COSO internal controls, 9
 - COSO internal controls risk assessment, 13
 - COSO monitoring, 17
 - human resources policies and practices, 12
 - integrity and ethical values, 10
 - internal controls definition, 8
 - internal controls standards background, 8
 - management philosophy and operating style, 11
 - monitoring, 17
 - monitoring design and implementation processes, 21
 - organizational structure, 12
 - other dimensions of the COSO internal controls, 20
 - reporting internal control deficiencies, 19
 - risk assessment, 13
 - Sarbanes-Oxley Act (SOx), 22
 - Treadway Commission, 8
- COSO internal controls
 - CobiT to assess internal controls, 40
 - COSO ERM framework, 97, 100
 - COSO internal control framework, 9
 - good internal controls summary, 6
 - internal controls standards background, 7
 - SOx internal controls review procedures, 4
- COSO internal controls framework
 - audit professional responsibilities, 3
 - CobiT framework, 36
- COSO internal controls risk assessment
 - COSO internal control framework, 13
- COSO internal control standards
 - audit professional responsibilities, 4
- COSO monitoring
 - COSO internal control framework, 17
 - internal control evaluation process, 18
 - physical inventories and asset reconciliation., 17
- CQA examination and requirements
 - certified quality auditors (CQA), 630
- Credit card fraud
 - IT-related laws, 394
- Cybersecurity internal controls audit
 - procedures
 - IT audit procedures, 449
- D**
 - Dashboard monitoring approaches
 - continuous assurance auditing (CAA), 337
 - Data and document classification processes
 - document classification procedures, 515
 - Data archival policies
 - document classification procedures, 512
 - Data archiving processes
 - electronic data records management, 509
 - electronic document management processes, 511
 - electronic records documentation retention, 516
 - Data profiling privacy issues
 - IT security controls, 443
 - Data warehouses and data mining
 - IT audit procedures, 341
 - Delivery and support control objectives
 - CobiT to assess internal controls, 45
 - Deming's PDCA cycle
 - monitoring and evaluation (ME) control objectives, 49
 - navigating the CobiT framework, 49
 - Design-measure-analyze-improve-control (DMAIC)
 - six sigma background and concepts, 579
 - six sigma process improvements, 579
 - Desktop and laptop systems DRP processes
 - IT emergency response plans, 496
 - Detection risk
 - risk management fundamentals, 84
 - Developing and processing CAATTs
 - ACL CAATT example, 319
 - CAATT software tools, 311
 - computer-assisted audit techniques, 309
 - continuous audit monitor example, 332
 - IT audit procedures, 307
 - programming steps for developing a CAATT application, 316
 - test data application tests, 320
 - test deck objectives, 320
 - Developing effective BCM strategies
 - business continuity development processes, 533
 - Disaster plan review IT audit procedures
 - IT audit procedures, 507
 - Disaster recovery business failure impact analysis
 - high availability analytics, 505
 - internal audit disaster recovery plan reviews, 500
 - Disaster recovery emergency handling
 - DRP deliverables, 502
 - Discovery sampling
 - audit sampling approaches, 137
 - DMAIC procedures
 - six sigma projects, 586

- Document classification procedures
 - data and document classification processes, 515
 - data archival policies, 512
 - enterprise document classification categories, 514
 - Document metadata
 - electronic data archiving, 518
 - relationship of metadata to individual file records, 518
 - DRP client-server readiness reviews
 - business impact analysis, 498
 - IT audit procedures, 493
 - DRP deliverables
 - building a DRP, 498
 - disaster recovery emergency handling, 502
 - Due professional care
 - IPPF IIA internal audit standards, 68
- E**
- Effective security environment using GASSP
 - GASSP principles, 428
 - Electronic data archiving
 - document metadata, 518
 - electronic records documentation retention, 517
 - Electronic data records management
 - data archiving processes, 509
 - electronic document control policies, 511
 - Electronic documentation standards
 - Association for Information and Image Management, 516
 - Electronic document control policies
 - electronic data records management, 511
 - electronic document security policies, 513
 - Electronic document management processes
 - data archiving processes, 511
 - Electronic document security policies
 - electronic document control policies, 513
 - Electronic records documentation retention
 - data archiving processes, 516
 - electronic data archiving, 517
 - Electronic records management internal controls
 - IT audit procedures, 300
 - Emergency change and patch management processes
 - IT internal control procedures, 565
 - Enterprise document classification categories
 - document classification procedures, 514
 - Enterprise risk management definition
 - COSO ERM framework, 97
 - Enterprise risks
 - Bhopal gas leak, 91
 - key risk assessment principles, 88, 89
 - risk management process, 87
 - Entity-level risks
 - business unit entity-level risks, 113
 - COSO ERM framework, 112
 - Estimating continuity requirements
 - continuity requirements analysis, 529
 - Evaluating attributes sampling test results
 - attributes sampling tests, 141
 - Event identification
 - COSO ERM framework, 103
 - Evolving control issues
 - cloud computing concepts, 220
 - IT audit objectives for data warehouse environments, 343
 - IT wireless networks, 215
 - online analytical processing (OLAP), 344
 - storage virtualization, 225
 - XBRL, 346
 - Excuses and reasons for committing fraud
 - red flags indicating risk of potential financial fraud, 460
- F**
- File transfer protocol software (FTP)
 - IT operating system fundamentals, 211
 - Firewalls
 - IT network components, 548
 - Fraud detection and prevention
 - Association of Certified Fraud Examiners (ACFE), 454
 - fraud risk assessment framework, 466
 - IIA standards for detecting and investigating fraud, 463
 - ISACA materials for detecting and investigating fraud, 463
 - IT audit procedures, 455
 - red flag fraud detection warnings, 456
 - red flags indicating risk of potential financial fraud, 458
 - SAS No. 99 auditor responsibility for detecting financial fraud, 461
 - Fraud risk assessment framework
 - fraud detection and prevention, 466
 - Fully mirrored recovery operations
 - building a DRP, 500
 - IT disaster recovery planning processes, 505
- G**
- GASSP principles
 - effective security environment using GASSP, 428
 - generally accepted systems security principles (GASSP), 424
 - Generalized audit software
 - computer-assisted audit tools and techniques (CAATT), 311

- Generally accepted systems security principles (GASSP)
 - GASSP principles, 424
 - IT security standards, 424
 - GLBA financial privacy rules
 - Gramm-Leach-Bliley Act (GLBA), 390
 - GLBA pretexting provisions
 - Gramm-Leach-Bliley Act (GLBA), 393
 - GLBA safeguards rule
 - Gramm-Leach-Bliley Act (GLBA), 392
 - Good internal controls summary
 - COSO internal controls, 6
 - Gramm-Leach-Bliley Act (GLBA)
 - GLBA financial privacy rules, 390
 - GLBA pretexting provisions, 393
 - GLBA safeguards rule, 392
 - IT-related laws, 390
 - pretexting, 393
- H**
- High availability analytics
 - disaster recovery business failure impact analysis, 505
 - HIPAA
 - HIPAA patient record privacy rules, 396
 - HIPAA security administrative procedures, 400
 - HIPAA cryptography and security requirements, 398
 - IT-related laws, 395
 - HIPAA patient record privacy rules
 - HIPAA, 396
 - HIPAA security administrative procedures
 - HIPAA, 400
 - HIPAA cryptography and security requirements
 - HIPAA, 398
 - Hot site facilities
 - building a DRP, 500
 - Human resources policies and practices
 - COSO internal control framework, 12
- I**
- Identity and access management key concepts
 - processes for managing access to enterprise IT resources, 474
 - Identity and access management processes
 - password verification controls, 473
 - processes for managing access to enterprise IT resources, 472
 - IIA code of ethics
 - IIA standards, 80
 - IIA international standards
 - IIA risk-related international standards, 94
 - IIA red book standards
 - IPPF IIA internal audit standards, 59
 - IIA risk-related International standards
 - IIA international standards, 94
 - IIA risk-related international standards
 - internal audit performance standards, 69
 - IIA standards
 - IIA code of ethics, 80
 - IIA standards for detecting and investigating fraud, 463
 - IPPF IIA internal audit standards, 57
 - IIA standards for detecting and investigating fraud
 - fraud detection and prevention, 463
 - IIA standards, 463
 - IIA standards practice advisories
 - IPPF IIA internal audit standards, 75
 - Impact analysis criteria
 - business impact analysis, 528
 - Implementing continuous assurance auditing
 - IT audit procedures, 330
 - Implementing improved IT governance
 - Val IT, 369
 - Incident management plans
 - business continuity development processes, 535
 - Incident response structures
 - business continuity development processes, 535
 - Independence and objectivity internal audit standards
 - IPPF IIA internal audit standards, 61
 - Information and communication
 - COSO ERM framework, 108
 - Information technology assurance framework (ITAF)
 - ISACA standards, 54
 - Information technology infrastructure library (ITIL)
 - ITIL continuous feedback loop, 178
 - ITIL service design, 181
 - ITIL service strategies, 179
 - IT Infrastructure controls, 176
 - Inherent risk definition
 - risk management fundamentals, 84
 - Integrity and ethical values
 - codes of conduct, 10
 - COSO internal control framework, 10
 - Internal audit attribute standards
 - IPPF IIA internal audit standards, 64
 - Internal audit BCM self-assessment reviews
 - IT audit procedures, 540
 - Internal audit charters
 - internal audit procedures, 593
 - performing effective IT audits, 118
 - Internal audit disaster recovery plan reviews
 - auditing a disaster recovery plan (DRP), 491
 - disaster recovery business failure impact analysis, 500
 - IT emergency response plans, 493

- Internal audit functions
 - CAE responsibilities, 595
 - IT audit specialists, 596
 - role of chief audit executive (CAE), 595
- Internal audit organization chart
 - internal audit procedures, 603
- Internal audit performance standards
 - IIA risk-related international standards, 69
- Internal audit procedures
 - internal audit charters, 593
 - internal audit organization chart, 603
- Internal audit reviews of enterprise BCM processes
 - IT audit procedures, 542
- Internal audit's role
 - section 404 internal controls reviews, 28, 29
- Internal audit standards objectives
 - IPPF IIA internal audit standards, 58
- Internal control evaluation process
 - benchmarking, 18
 - COSO monitoring, 18
- Internal controls definition
 - COSO internal control framework, 8
- Internal controls standards background
 - COSO internal control framework, 8
 - COSO internal controls, 7
 - IT audit roles and responsibilities, 7
 - SAS No. 1, 7
 - treadway commission, 7
- Internal ISMS audits
 - ISO 27001, 637
- International information systems security certification consortium
 - certified information system security professional (CISSP), 628
- International standards
 - XBRL defined, 347
- International Standards Organization (ISO)
 - ISO standards overview, 407
- International standards professional practices framework
 - IPPF IIA internal audit standards, 62
- Intrusion detection IT audit control procedures
 - IT audit procedures, 553
 - IT network security controls, 553
- Intrusion detection terminology, 551
- IPPF IIA internal audit standards
 - due professional care, 68
 - IIA red book standards, 59
 - IIA standards, 57
 - IIA standards practice advisories, 75
 - independence and objectivity internal audit standards, 61
 - internal audit attribute standards, 64
 - internal audit standards objectives, 58
 - international standards professional practices framework, 62
 - managing the internal audit activity, 69
- Irregularities and illegal acts
 - ISACA standards, 404
- ISACA audit risk-related standards
 - ISACA standards, 95
- ISACA code of professional ethics
 - ISACA standards, 81
- ISACA IT auditing standards
 - ISACA standards, 76
- ISACA materials for detecting and investigating fraud
 - fraud detection and prevention, 463
 - ISACA standards, 463
- ISACA standards
 - CobIT, 32
 - information technology assurance framework (ITAF), 54
 - irregularities and illegal acts, 404
 - ISACA audit risk-related standards, 95
 - ISACA code of professional ethics, 81
 - ISACA IT auditing standards, 76
 - ISACA materials for detecting and investigating fraud, 463
 - IT zone (ITGI), 32
 - Val IT, 363
- ISO 27001
 - internal ISMS audits, 637
 - IT security technique requirements, 417
- ISO 27002
 - BS 25999 good practice guidelines, 543
- ISO documentation hierarchy
 - ISO standards overview, 414
- ISO 19011 IT audit standards outline
 - ISO standards overview, 420
- ISO IT security standards: ISO 17799 and 27001
 - ISO standards overview, 415
 - ISO 27002 standards topics, 416
- ISO 9001 quality management systems
 - ISO standards overview, 411
 - quality management system process, 413
- ISO 19011 quality management systems auditing
 - ISO standards overview, 419
- ISO 20000 service quality management
 - ISO standards overview, 418
- ISO standards overview
 - International Standards Organization (ISO), 407
 - ISO documentation hierarchy, 414
 - ISO 19011 IT audit standards outline, 420
 - ISO IT security standards: ISO 17799 and 27001, 415
 - ISO 9001 quality management systems, 411

- ISO standards overview (*continued*)
 - ISO 19011 quality management systems auditing, 419
 - ISO 20000 service quality management, 418
 - ISO 27002 standards topics
 - ISO IT security standards: ISO 17799 and 27001, 416
- IT application change and patch management controls
 - IT audit procedures, 566
- IT application change management processes
 - categories of IT application changes and patches, 565
 - change management metric measures, 568
 - IT internal control procedures, 561
- IT application controls
 - application selection risk factors, 240
 - IT audit procedures, 230
- IT application patch management processes
 - IT audit procedures, 434
- IT application review audit procedures
 - application controls reviews, 249
- IT application review processing controls
 - application controls reviews, 251
- IT audit cybersecurity and privacy controls
 - IT audit procedures, 434
- IT audit function quality assurance reviews
 - benefits of IT audit quality-assurance reviews, 642
 - IT audit procedures, 641
 - standards for the professional practice of internal auditing, 641
- IT audit functions
 - IT audit manager position description, 599
 - IT audit procedures, 600
- IT audit guidelines for XBRL processes
 - IT audit procedures, 350
- IT auditing standards
 - IT audit procedures, 600
- IT audit manager position description
 - IT audit functions, 599
- IT audit objectives
 - performing effective IT audits, 122
- IT audit objectives for data warehouse environments
 - evolving control issues, 343
 - IT audit procedures, 343
- IT auditor
 - IT audit roles and responsibilities, 4
- IT auditor basic knowledge requirements
 - IT audit specialists, 597
- IT auditor "best evidence" classification
 - audit evidence, 133
- IT auditor data center disaster recovery plan reviews
 - IT audit procedures, 490
- IT audit organization
 - performing effective IT audits, 121
- IT auditor identity and access management procedures
 - IT audit procedures, 472
- IT auditor job description
 - IT audit roles and responsibilities, 5
- IT auditor responsibilities
 - role of audit committee, 356
- IT auditor responsibility
 - codes of conduct, 10
- IT auditor review points
 - SOA service aggregator concepts, 285
- IT audit plans
 - performing effective IT audits, 124
 - role of audit committee, 359
- IT audit procedures
 - application control elements, 230
 - application controls reviews, 242
 - application development review guidelines, 237
 - application tests of compliance, 257
 - auditing a disaster recovery plan (DRP), 489
 - auditing BCM processes, 540
 - auditing change and patch management procedures, 573
 - auditing COSO ERM, 114
 - auditing electronic document management processes, 520
 - auditing enterprise BCM processes, 541
 - auditing Gramm-Leach-Bliley Act compliance, 395
 - auditing HIPAA requirements procedures, 399
 - auditing identity and access management processes, 484
 - auditing service-oriented architectures, 296
 - auditing SOA environments, 294
 - auditing SOA governance general controls, 296
 - auditing web services applications, 298
 - automated identity and access management processes, 475
 - business continuity plan requirements, 537
 - CAATT objectives, 307
 - cloud computing application controls, 222
 - cloud computing service provider selection, 224
 - CMMI IT audit processes, 281
 - components of a DRP, 489
 - computer-assisted audit tools and techniques (CAATT), 305
 - continuous assurance auditing, 339
 - cybersecurity internal controls audit procedures, 449
 - data warehouses and data mining, 341
 - developing and processing CAATTs, 307
 - disaster plan review IT audit procedures, 507

- DRP client-server readiness reviews, 493
- electronic records management internal controls, 300
- fraud detection and prevention, 455
- implementing continuous assurance auditing, 330
- internal audit BCM self-assessment reviews, 540
- internal audit reviews of enterprise BCM processes, 542
- intrusion detection IT audit control procedures, 553
- IT application change and patch management controls, 566
- IT application controls, 230
- IT application patch management processes, 560
- IT audit cybersecurity and privacy controls, 434
- IT audit function quality assurance reviews, 641
- IT audit functions, 600
- IT audit guidelines for XBRL processes, 350
- IT auditing standards, 600
- IT audit objectives for data warehouse environments, 343
- IT auditor data center disaster recovery plan reviews, 490
- IT auditor Identity and access management procedures, 472
- IT audit steps for a review of VPN internal controls, 556
- IT audit workpaper security best practices, 452
- IT business continuity planning processes, 488
- IT change management procedures audit steps, 574
- IT disaster recovery planning processes, 486
- IT fraud investigations, 467
- IT fraud prevention processes, 468
- ITIL configuration management, 193
- ITIL problem management, 198
- IT infrastructure management, 199
- IT patch management controls, 569
- IT systems fraud risk assessments, 465
- organizing an IT audit function, 592
- organizing IT audit functions, 600
- patch testing, 571
- preimplementation auditing, 258
- preimplementation review objectives, 260
- project management processes, 375
- purchased software internal controls, 238
- reviewing IT access management processes, 477
- review of a six sigma program, 589
- reviews of electronic records document controls, 302
- SOA internal control issues and risks, 287
- unix general controls review procedures, 205
- wireless network vulnerabilities and risks, 218
- workpaper security, 450
- IT audit process steps
 - performing effective IT audits, 149
- IT audit program formats
 - performing effective IT audits, 127
- IT audit program steps
 - performing effective IT audits, 128
- IT audit quality-assurance reviews
 - quality-assurance reviews of IT audit activities, 644
- IT audit roles and responsibilities
 - internal controls standards background, 7
 - IT auditor, 4
 - IT auditor job description, 5
 - role of the IT auditor, 4
- IT audit significant findings
 - audit committee reports, 361
 - audit committee reviews, 360
- IT audit specialists
 - basic knowledge requirements, 597
 - internal audit functions, 596
 - IT auditor, basic knowledge requirements, 597
 - skill requirements, 597
- IT audit status reports
 - role of audit committee, 360
- IT audit steps for a review of VPN internal controls
 - IT audit procedures, 556
- IT audit tasks
 - COSO ERM, 113
- IT audit workpaper purposes
 - performing effective IT audits, 143
- IT audit workpapers
 - performing effective IT audits, 143
- IT audit workpaper security best practices
 - IT audit procedures, 452
- IT availability and costs relationships
 - service delivery availability management, 188
- IT business continuity planning processes
 - IT audit procedures, 488
- IT change management procedures audit steps
 - IT audit procedures, 574
- IT change management processes
 - IT internal control procedures, 559
- IT change management requirements
 - COSO ERM, 562
- IT disaster recovery planning processes
 - building a DRP, 497
 - business continuity plan training, 503
 - fully mirrored recovery operations, 505
 - IT audit procedures, 486
 - service level agreements (SLAs), 504

- IT emergency response plans
 - desktop and laptop systems DRP processes, 496
 - internal audit disaster recovery plan reviews, 493
- IT emergency response procedures
 - client-server IT process continuity planning, 495
- IT fraud investigations
 - IT audit procedures, 467
- IT fraud prevention processes
 - IT audit procedures, 468
- IT general and application controls hierarchy
 - IT general controls, 156
- IT general controls
 - client-server and smaller-systems general IT controls, 165
 - IT general and application controls hierarchy, 156
 - IT internal controls, 153
 - IT organization and management, 159
 - IT physical and environmental general controls, 159
 - IT standards, 158
 - IT technical environment general controls, 174
 - larger-system general controls review objectives, 164
 - performing effective IT audits, 153
 - preliminary survey review steps, 160
 - small business IT system controls, 167
- ITGI navigation framework
 - CobiT to assess internal controls, 40
- IT governance general controls
 - performing effective IT audits, 157
 - Sarbanes-Oxley Act (SOx), 157
- IT governance institute (ITGI)
 - ISACA standards, 32
 - Val IT, 363
- IT identity management processes
 - IT security controls, 476
- ITIL availability management
 - ITIL service management best practices, 187
- ITIL capacity management
 - capacity management sub processes, 186
 - ITIL service management best practices, 186
- ITIL configuration management
 - IT audit procedures, 193
- ITIL continuity management
 - business continuity and disaster recovery strategies, 189
 - ITIL service management best practices, 188
- ITIL continuous feedback loop
 - information technology infrastructure library (ITIL), 178
 - ITIL service management best practices, 178
- ITIL financial management sub processes
 - ITIL service management best practices, 179
- ITIL incident management
 - ITIL service management best practices, 194
 - service desk roles, 195
- ITIL incident management life cycle
 - ITIL service management best practices, 196
- ITIL information security objectives
 - service delivery information systems security management, 189
- ITIL problem management
 - IT audit procedures, 198
 - ITIL service management best practices, 196
- ITIL release management
 - ITIL service management best practices, 193
- ITIL service design
 - information technology infrastructure library (ITIL), 181
- ITIL service management best practices
 - CobiT references, 177
 - configuration management, 191
 - ITIL availability management, 187
 - ITIL capacity management, 186
 - ITIL continuity management, 188
 - ITIL continuous feedback loop, 178
 - ITIL financial management sub processes, 179
 - ITIL incident management, 194
 - ITIL incident management life cycle, 196
 - ITIL problem management, 196
 - ITIL release management, 193
 - ITIL service operations processes, 194
 - ITIL service transition change management, 190
- IT infrastructure controls, 176
- service delivery availability management, 187
- service delivery capacity management, 186
- service delivery continuity management, 188
- service delivery information systems security management, 189
- service delivery service level management, 182
- service-level agreements (SLAs), 183
- service operation event and incident management, 194
- service operation problem management, 196
- service transition change management, 190
- service transition configuration management, 191
- service transition release management, 193

- ITIL service operations processes
 - ITIL service management best practices, 194
- ITIL service strategies
 - information technology infrastructure library (ITIL), 179
- ITIL service transition change management
 - ITIL service management best practices, 190
 - IT internal controls, 191
- IT infrastructure controls
 - information technology infrastructure library (ITIL), 176
 - ITIL service management best practices, 176
- IT infrastructure management
 - IT audit procedures, 199
- IT internal auditor knowledge requirements
 - performing effective IT audits, 122
- IT internal control procedures
 - change and patch management control processes, 558
 - emergency change and patch management processes, 565
 - IT application change management processes, 561
 - IT change management processes, 559
 - IT preventive, detective, and corrective change controls, 566
- IT internal controls
 - IT general controls, 153
 - ITIL service transition change management, 191
 - IT wireless networks, 215
- IT investments
 - Val IT, 364
- IT management general controls
 - performing effective IT audits, 158
- IT network components
 - firewalls, 548
 - IT network security controls, 549
 - IT telecommunications systems and networks, 545
 - network routers, 547
 - VPN firewall configurations, 554
- IT network security controls, 550
 - Intrusion detection IT audit control procedures, 553
 - intrusion detection terminology, 550
 - IT network components, 549
 - virtual private networks, 552
 - VPN risks, 554
- IT network security fundamentals
 - IT security controls, 435
 - IT system firewalls, 441
 - IT systems privacy controls, 443
 - phishing identity threats, 440
 - radio frequency identification security issues, 444
 - viruses and malicious program code, 439
- IT operating system fundamentals
 - cloud computing concepts, 220
 - file transfer protocol software (FTP), 211
 - IT operations general controls, 202
 - IT wireless system components, 217
 - operating system features, 206
 - OS general functions, 207
 - role of the computer operating system, 203
 - systems software, 202
 - virtual memory management concepts, 208
 - virus protection software, 211
 - wireless network architecture, 217
- IT operations general controls
 - IT operating system fundamentals, 202
- IT organization and management
 - IT general controls, 159
- IT password logon exchanges
 - security of data concepts, 438
- IT patch management controls
 - IT audit procedures, 569
 - patch installation and deployment, 571
 - security and patch information requirements, 570
- IT perimeter security
 - top-down IT security model, 430
- IT physical and environmental general controls
 - IT general controls, 159
- IT portfolio management
 - Val IT, 364
 - Val IT initiative, 371
- IT preventive, detective, and corrective change controls
 - IT internal control procedures, 566
- IT program management
 - Val IT initiative, 371
- IT-related laws
 - Computer Fraud and Abuse Act (CFAA), 386
 - Computer Security Act of 1987, 388
 - credit card fraud, 394
 - Gramm-Leach-Bliley Act (GLBA), 390
 - HIPAA, 395
- IT resources
 - CobIT cube components, 37, 38
- IT security controls
 - authentication and authorization processes, 479
 - data profiling privacy issues, 443
 - IT identity management processes, 476
 - IT network security fundamentals, 435
 - malicious program code types, 440
 - PCI-DSS requirements, 446
 - perimeter security classifications for interconnected systems, 431
 - security of data concepts, 437
 - separation of duties identity management controls, 477
 - systems firewall configurations, 441

662 ■ Index

- IT security standards
 - generally accepted systems security principles (GASSP), 424
 - IT security technique requirements
 - ISO 27001, 417
 - IT standards
 - IT general controls, 158
 - IT system administration processes
 - processes for managing access to enterprise IT resources, 474
 - IT system firewalls
 - IT network security fundamentals, 441
 - IT systems fraud risk assessments
 - IT audit procedures, 465
 - IT systems privacy controls
 - IT network security fundamentals, 443
 - IT technical environment general controls
 - IT general controls, 174
 - IT telecommunications systems and networks
 - IT network components, 545
 - key security risks, internal controls and best practices, 544
 - IT value management initiatives
 - Val IT framework principles, 367
 - IT value management readiness assessments
 - Val IT, 368
 - IT wireless networks
 - control and security characteristics, 216
 - evolving control issues, 215
 - IT internal controls, 215
 - IT wireless system components
 - IT operating system fundamentals, 217
 - wireless network security concerns, 219
- J**
- Joint probability formula
 - key risk assessment principles, 90
- K**
- Key risk assessment principles
 - enterprise risks, 88, 89
 - joint probability formula, 90
 - quantitative risk assessment techniques, 92
 - risk independencies, 90
 - risk ranking expected cost estimates, 93
 - risk scoring schedules, 91
 - Key security risks, internal controls and best practices
 - IT telecommunications systems and networks, 544
 - virtual private networks, intrusion detection, & internal controls., 545
 - KPA status review IT audit procedures
 - CMMi, 275
- L**
- Larger-system general controls review
 - objectives
 - IT general controls, 164
 - Lean six sigma
 - lean six sigma IT processes, 588
 - lean technologies, 587
 - Lean six sigma IT processes
 - lean six sigma, 588
 - Lean technologies
 - lean six sigma, 587
 - Legal and regulatory compliance risk objectives
 - COSO ERM framework, 110
- M**
- Maintaining CIA certifications
 - CIA examination, 623
 - Major disaster recovery threats
 - risk assessments, 534
 - Malicious program code types
 - IT security controls, 440
 - Management philosophy and operating style
 - COSO internal control framework, 11
 - Managing internal audit activity
 - IPPF IA internal audit standards, 69
 - Microsoft CAA approach
 - TECA implementation at microsoft, 336
 - Monitoring
 - COSO internal control framework, 17
 - Monitoring and evaluation (ME) control objectives
 - capability maturity model for integration (CMMi), 51
 - CobiT to assess internal controls, 48
 - Deming's PDCA cycle, 49
 - Monitoring design and implementation processes
 - COSO internal control framework, 21
- N**
- National Institute of Science and Technology (NIST)
 - NIST audit and accountability published documents, 389
 - National institute of science and technology (NIST)
 - Computer Security Act of 1987, 388
 - Navigating the CobiT framework
 - CobiT to assess internal controls, 41
 - Deming's PDCA cycle, 49
 - Network routers
 - IT network components, 547
 - NIST audit and accountability published documents
 - national institute of science and technology (NIST), 389

O

- Object-oriented programming language
 - concepts
 - computer program architectures, 236
- OLAP software features
 - online analytical processing (OLAP), 345
- Online analytical processing (OLAP)
 - evolving control issues, 344
 - OLAP software features, 345
- Operating system features
 - IT operating system fundamentals, 206
- Organizational structure
 - COSO internal control framework, 12
- Organizing an IT audit function
 - IT audit procedures, 592
 - standards for the professional practice of internal auditing, 592
- Organizing IT audit functions
 - audit program preparation procedures, 601
 - IT audit procedures, 600
- OS general functions
 - IT operating system fundamentals, 207
- Other dimensions of the COSO internal controls
 - COSO internal control framework, 20

P

- Pareto chart example
 - quality audit division (QAD), 637
- Password verification controls
 - identity and access management processes, 473
- Patch installation and deployment
 - IT patch management controls, 571
- Patch testing
 - IT audit procedures, 571
- Payment card industry (PCI) council
 - PBI-DSS standards and controls, 446
- PBI-DSS standards and controls
 - payment card industry (PCI) council, 446
- PCAOB
 - Sarbanes-Oxley Act (SOx), 24
- PCI-DSS requirements
 - IT security controls, 446
- PDCA cycle
 - performing ASQ quality audits, 639
- Performing an application walkthrough
 - application controls reviews, 245
- Performing ASQ quality audits
 - PDCA cycle, 639
 - quality audit process steps, 640
- Performing effective IT audits
 - applications review IT audit plan, 125
 - audit evidence, 132
 - audit planning memo, 124
 - audit programs, 125
 - audit sampling approaches, 133
 - audit sampling benefits, 135
 - checklist format audit programs, 129
 - internal audit charters, 118
 - IT audit objectives, 122
 - IT audit organization, 121
 - IT audit plans, 124
 - IT audit process steps, 149
 - IT audit program formats, 127
 - IT audit program steps, 128
 - IT audit workpaper purposes, 143
 - IT audit workpapers, 143
 - IT general controls, 153
 - IT governance general controls, 157
 - IT internal auditor knowledge requirements, 122
 - IT management general controls, 158
 - workpaper documentation, 145
- Perimeter security classifications for interconnected systems
 - IT security controls, 431
- Permanent files
 - workpaper documentation, 145
- Phishing identity threats
 - IT network security fundamentals, 440
- Physical inventories and asset reconciliation.
 - COSO monitoring, 17
- Planning and organizing (PO) control objectives
 - CobIT to assess internal controls, 41
- PMBOK guidance
 - project, program, and portfolio interactions, 373
 - project management institute (PMI), 376
 - project management knowledge areas, 377
 - project management plan data flow diagram, 382
 - Project management process groups, 377
- PMBOK processes
 - project management knowledge areas, 379
- Post implementation review objectives
 - application controls reviews, 264
- Preimplementation auditing
 - IT audit procedures, 258
- Preimplementation review objectives
 - IT audit procedures, 260
- Preimplementation review problems
 - applications under development, 261
- Preimplementation review procedures
 - applications under development, 262
- Preliminary survey review steps
 - IT general controls, 160
- Pretexting
 - Gramm-Leach-Bliley Act (GLBA), 393

- Processes for managing access to enterprise IT resources
 - access management provisioning processes, 478
 - identity and access management key concepts, 474
 - identity and access management processes, 472
 - IT system administration processes, 474
 - Professional certifications
 - certified information systems auditor (CISA), 607
 - Programming steps for developing a CAATT application
 - developing and processing CAATTs, 316
 - Project, program, and portfolio interactions
 - PMBOK guidance, 373
 - Project management book of knowledge (PMBOK)
 - project management institute (PMI), 376
 - Project management institute (PMI)
 - PMBOK guidance, 376
 - project management book of knowledge, 376
 - Project management knowledge areas
 - PMBOK guidance, 377
 - PMBOK processes, 379
 - Project management plan data flow diagram
 - PMBOK guidance, 382
 - Project management plan development
 - project management processes, 380
 - Project management processes
 - IT audit procedures, 375
 - project management plan development, 380
 - Project management process groups
 - PMBOK guidance, 377
 - Public Company Accounting Oversight Board
 - Sarbanes-Oxley Act (SOx), 24
 - Purchased software internal controls
 - IT audit procedures, 238
- Q**
- Quality-assurance reviews of IT audit activities
 - IT audit quality-assurance reviews, 644
 - Quality audit classifications
 - third-party audits., 634
 - Quality audit division (QAD)
 - American Society for Quality (ASQ), 633
 - Pareto chart example, 637
 - Quality auditor responsibilities
 - certified quality auditors (CQA), 633
 - Quality audit process steps
 - performing ASQ quality audits, 640
 - Quality audit types
 - certified quality auditors (CQA), 636
 - Quality management system process
 - ISO 9001 quality management systems, 413
 - Quantitative risk assessment techniques
 - key risk assessment principles, 92
- R**
- RACI charts
 - CobiT to assess internal controls, 42
 - Radio frequency identification security issues
 - IT network security fundamentals, 444
 - Red flag fraud detection warnings
 - fraud detection and prevention, 456
 - Red Flags Indicating risk of potential financial fraud
 - fraud detection and prevention, 458
 - Red flags indicating risk of potential financial fraud
 - excuses and reasons for committing fraud, 460
 - Relationship of metadata to individual file records
 - document metadata, 518
 - Report generator LLanguage characteristics
 - report generators languages, 317
 - Report generatorslanguages
 - CAATT software tools, 316
 - report generator language characteristics, 317
 - Reporting internal control deficiencies
 - COSO internal control framework, 19
 - Residual risk definition
 - risk management fundamentals, 84
 - Reviewing IT access management processes
 - IT audit procedures, 477
 - Review of a six sigma program
 - IT audit procedures, 589
 - Reviews of electronic records document controls
 - IT audit procedures, 302
 - Risk appetite
 - COSO ERM framework, 98
 - risk management fundamentals, 98
 - Risk appetite map
 - risk management fundamentals, 103
 - Risk assessment
 - COSO internal control framework, 13
 - Risk assessment process steps
 - business impact analysis, 531
 - Risk assessments
 - business continuity management, 530
 - COSO ERM framework, 104
 - major disaster recovery threats, 534
 - Risk identification
 - risk management process, 85
 - Risk independencies
 - key risk assessment principles, 90

- Risk management fundamentals
 - COSO ERM, 83
 - detection risk, 84
 - inherent risk, 84
 - residual risk, 84
 - risk appetite, 98
 - risk appetite map, 103
 - risk management process, 85
 - Risk management objectives
 - COSO ERM framework, 109
 - Risk management process
 - enterprise risks, 87
 - risk identification, 85
 - risk management fundamentals, 85
 - Risk ranking expected cost estimates
 - key risk assessment principles, 93
 - Risk response strategies
 - COSO ERM framework, 105
 - Risk scoring schedules
 - key risk assessment principles, 91
 - Role of audit committee
 - IT auditor responsibilities, 356
 - IT audit plans, 359
 - IT audit status reports, 360
 - SOx audit committee requirements, 356
 - Role of chief audit executive (CAE)
 - internal audit functions, 595
 - Role of the computer operating system
 - IT operating system fundamentals, 203
 - Role of the IT auditor
 - IT audit roles and responsibilities, 4
- S**
- Sarbanes-Oxley Act (SOx)
 - COSO internal control framework, 22
 - IT governance general controls, 157
 - public company accounting oversight board, 24
 - Sarbanes-Oxley Act key provisions
 - summary, 23
 - section 404 compliance review, 27
 - section 404 internal controls assessments, 26
 - SOx key elements, 22
 - SOx section 404, 24
 - Sarbanes-Oxley Act key provisions summary
 - Sarbanes-Oxley Act (SOx), 23
 - SAS No. 1
 - auditing standards, 7
 - internal controls standards background, 7
 - SAS No. 99 auditor responsibility for detecting financial fraud
 - fraud detection and prevention, 461
 - Section 404 compliance review
 - Sarbanes-Oxley Act (SOx), 27
 - Section 404 internal controls assessments
 - Sarbanes-Oxley Act (SOx), 26
 - Section 404 internal controls review
 - AS5 objectives, 29
 - Section 404 internal controls reviews, 29
 - CobiT to assess internal controls, 51
 - internal audit's role, 28, 29
 - Security and patch information requirements
 - IT patch management controls, 570
 - Security of data concepts
 - IT password logon exchanges, 438
 - IT security controls, 437
 - Separation of duties identity management controls
 - IT security controls, 477
 - Service delivery availability management
 - IT availability and costs relationships, 188
 - ITIL service management best practices, 187
 - Service delivery capacity management
 - ITIL service management best practices, 186
 - Service delivery continuity management
 - ITIL service management best practices, 188
 - Service delivery information systems security management
 - ITIL information security objectives, 189
 - ITIL service management best practices, 189
 - Service delivery service level management
 - ITIL service management best practices, 182
 - Service desk roles
 - ITIL incident management, 195
 - Service-level agreement contents
 - service-level agreements (SLAs), 184
 - Service-level agreements
 - SOA policies and procedures, 293
 - Service level agreements (SLAs)
 - IT disaster recovery planning processes, 504
 - Service-level agreements (SLAs)
 - ITIL service management best practices, 183
 - service-level agreement contents, 184
 - Service operation event and incident management
 - ITIL service management best practices, 194
 - Service operation problem management
 - ITIL service management best practices, 196
 - Service-oriented architecture (SOA)
 - SOA enterprise-wide configurations, 286
 - SOA internal control issues and risks, 287
 - SOA key benefits, 289
 - SOA policies and procedures, 290
 - SOA service aggregator concepts, 285
 - software engineering concepts, 283
 - web services architecture components, 299

- Service transition change management
 - ITIL service management best practices, 190
 - Service transition configuration management
 - ITIL service management best practices, 191
 - Service transition release management
 - ITIL service management best practices, 193
 - SIPOC charts
 - six sigma process improvements, 585
 - Six sigma
 - black belt body of knowledge, 583
 - six sigma background and concepts, 577
 - Six sigma deployment and process goals, 581
 - statistical quality control procedures, 577
 - Six sigma background and concepts
 - design-measure-analyze-improve-control (DMAIC), 579
 - six sigma, 577
 - Six sigma black belts
 - six sigma leadership roles, 582
 - Six sigma deployment and process goals
 - six sigma, 581
 - Six sigma leadership roles
 - six sigma black belts, 582
 - Six sigma process improvements
 - design-measure-analyze-improve-control (DMAIC), 579
 - SIPOC charts, 585
 - Six sigma projects
 - DMAIC procedures, 586
 - Skill requirements
 - IT audit specialists, 597
 - Small-business computer system program
 - library controls
 - small business IT system controls, 172
 - Small business IT system controls
 - IT general controls, 167
 - small-business computer system program
 - library controls, 172
 - SOA enterprise-wide configurations
 - service-oriented architecture (SOA), 286
 - SOA internal control issues and risks
 - IT audit procedures, 287
 - service-oriented architecture (SOA), 287
 - SOA key benefits
 - service-oriented architecture (SOA), 289
 - SOA policies and procedures
 - service-level agreements, 293
 - service-oriented architecture (SOA), 290
 - SOA service aggregator concepts
 - IT auditor review points, 285
 - service-oriented architecture (SOA), 285
 - Software as a service (SaaS)
 - cloud computing concepts, 221
 - Software engineering concepts
 - CMMi, 267
 - CMMi maturity levels, 270
 - service-oriented architecture (SOA), 283
 - Software engineering institute capability maturity model
 - CMMi, 267
 - SOx audit committee requirements
 - role of audit committee, 356
 - SOx internal controls review procedures
 - COSO internal controls, 4
 - SOx key elements
 - Sarbanes-Oxley Act (SOx), 22
 - SOx section 404
 - Sarbanes-Oxley Act (SOx), 24
 - Standards for the professional practice of internal auditing
 - IT audit function quality assurance reviews, 641
 - organizing an IT audit function, 592
 - Statistical quality control procedures
 - six sigma, 577
 - Storage virtualization
 - evolving control issues, 225
 - Systems development activities
 - CMMi level 1, 272
 - Systems firewall configurations
 - IT security controls, 441
 - Systems software
 - IT operating system fundamentals, 202
- T**
- TECA implementation at microsoft
 - microsoft CAA approach, 336
 - Test data application tests
 - developing and processing CAATs, 320
 - Test data CAATT approach
 - computer-assisted audit tools and techniques (CAATT), 322
 - Test deck approaches
 - computer-assisted audit tools and techniques (CAATT), 320
 - Test deck objectives
 - developing and processing CAATs, 320
 - Testing audit control objectives
 - application controls reviews, 249
 - Testing BCM plans
 - business continuity management, 538
 - Tests of application inputs and outputs
 - application controls reviews, 252
 - Third-party audits
 - quality audit classifications, 634
 - Top-down IT security model
 - IT perimeter security, 430
 - Treadway Commission
 - COSO internal control framework, 8
 - internal controls standards background, 7
- U**
- Unix general controls review procedures
 - IT audit procedures, 205

V

- Val IT
 - implementing improved IT governance, 369
 - ISACA standards, 363
 - IT governance institute (ITGI), 363
 - IT investments, 364
 - IT portfolio management, 364
 - IT value management readiness assessments, 368
- Val IT framework
 - Val IT initiative, 365
- Val IT framework principles
 - IT value management initiatives, 367
- Val IT guidance materials
 - CobiT framework, 365
- Val IT initiative
 - IT portfolio management, 371
 - IT program management, 371
 - Val IT framework, 365
- Variables sampling
 - audit sampling approaches, 136
- Virtual memory management concepts
 - IT operating system fundamentals, 208
- Virtual private networks
 - IT network security controls, 552
- Virtual private networks, intrusion detection, & internal controls.
 - key security risks, internal controls and best practices, 545
- Viruses and malicious program code
 - IT network security fundamentals, 439

- Virus protection software
 - IT operating system fundamentals, 211
- VPN firewall configurations
 - IT network components, 554
- VPN risks
 - IT network security controls, 554

W

- Web services applications
 - application controls reviews, 295
- Web services architecture components
 - service-oriented architecture (SOA), 299
- Wireless network architecture
 - IT operating system fundamentals, 217
- Wireless network security concerns
 - IT wireless system components, 219
- Wireless network vulnerabilities and risks
 - IT audit procedures, 218
- Workpaper documentation
 - audit procedures files, 147
 - performing effective IT audits, 145
 - permanent files, 145
 - workpaper point sheets, 148
- Workpaper point sheets
 - workpaper documentation, 148
- Workpaper security
 - IT audit procedures, 450

X

- XBRL
 - definition, international standards, 347
 - evolving control issues, 346

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>