

Index

Page references followed by *t* indicate a table

- A
- Access controls, 233
 - purchasing/ordering, 108
- Access requests, 233
- Accountability, structure, 35
- Accounting Standards Codification (ASC), Topic 985, 322
- Account reviews, 69
- Accounts payable (AP), 116–119
 - cost/process metrics, 104–105
 - internal control standard, 116–118
 - P2P automation solutions, 102
 - risk, 119
 - self-audit tools, 101
- Accounts receivable (AR), 49, 72–75
 - aging (metric), 51, 73
 - balance reviews, 76
 - internal control standard, 73–74
 - risk, 74–75
- Accrued revenue, 69
- Accuracy (control objective component), 32
- ACH payments, 122
- ACH supplier remittances, 100
- Adjusting entries, gross number (metric), 175
- Affirmative Action compliance, 192
- After-the-fact purchase orders, 110
- Agent fees, payment, 87
- Aging (metric), 51, 73
- American Accounting Association (AAA), 20
- American Institute of Certified Public Accountants (AICPA), 20, 24, 40
 - CPA Insider*, 42
- Annualized failure rates (AFRs), establishment, 305
- Application owner, 225
- AR
 - status/review (metric), 52
- Arm's-length principle, OECD
 - definition, 177–178
- Asset protection, 83, 271
 - company asset protection, 272
 - internal control, application, 273
 - metrics, 273
 - process, 271
 - sub-processes, 274
- Association of Certified Fraud Examiners (ACFE), Report to the Nations, 1
- Audit committee controls, 335–339
 - internal control standards, 336–338
 - risk, 338–339
- Audits, 169
- Authorization (control objective component), 32
- Authorized shipments, 65
- Automated matching, 99–100

- Automated workflow approvals, 100
- Available funds, investment, 92–94
 - internal control standard, 93
 - risk, 93–94
- B**
- Backbone, 242
- Balance adjustments, 73–74
- Balance of Payments Programs, 196
- Bank
 - account, limits, 121
 - payment, verification, 130
- Banking requirements, Treasury
 - controls, 89
- Bearer checks, 120
- Best possible DSO (metric), 52
- Billing
 - inputs, 73
 - transactions, 69
- Bills of Material (BOM), 165
- Blank check storage, 121
- Blanket purchase orders, 109
- Blank paper stock, usage, 71
- Blank payroll checks, security, 142
- Blank shipping forms, 66
- Bulletin boards, 264–269
 - internal control
 - standard, 266–268
 - risk, 268–269
- Business continuity
 - internal control standard/risk, 290
- Business continuity plan(ning),
 - 252–259, 342
 - internal control
 - standard, 257–258
 - risk, 258–259
- Business interruption contingency
 - plans, 107
- Business process
 - considerations, 253–254
 - understanding, 37
- Buy American Act, 196
- C**
- Call center management, 302–304
 - internal control
 - standard, 302–303
 - risk, 304
- Canadian Institute of Chartered Accountants (CICA), 24
- Capital transactions, 91
- Cardholder agreement, 130
- Cash
 - forecasts, accuracy, 87
 - petty cash, 122
 - pooling, 90
- Cash rebates/deductions, 64
 - advance, 69
- Cash receipts/application, 77–79
 - duties, segregation, 77
 - internal control standard, 77–78
 - risk, 78–79
- Cash-to-cash cycle time, 155
- CCL. *See* Commerce Control List
- Change management, 248–251
 - internal control
 - standard, 249–250
 - risk, 250–251
- Check 21
- Checks
 - blank payroll checks, security, 142
 - check-signing equipment, custody/
 - security, 122, 143
 - voided check procedures, 142
- Classification category, examples
 - (information type), 216t

- Clean Air/Water Acts, 192
- Cloud providers, 256
- Code of conduct, 174, 190, 208
 - components, 39–40
 - Institute of Business Ethics list, 39–40
 - considerations, 41
 - Treasury process, 86
- Collection, 75–76
 - internal control standard, 76
 - risk, 76
- Collection Effectiveness
 - Index (CEI), 52
- Collusion, 41
- Commerce Control List (CCL), 56
 - components, 57
- Committed credit, percentage, 87
- Committee of Sponsoring
 - Organizations of the Treadway Commission (COSO), 5, 20, 325
 - components, 21–22
 - Internal Control — Integrated Framework* (issuance), 29
 - monitoring guidance, 22–23
 - objectives, nonadherence, 335
- Communicated enterprise-level
 - objectives, 30–31
- Communication, 149
 - ERM component, 30
 - internal control system component, 21
 - method, 14
 - organization-level
 - communication, 31
 - senior management commitment/communication, 14
- Company
 - confidential/restricted, 209
 - securities, accounting, 89
- Compensating controls, 34
- Compensation/benefits, 145–147
 - internal control
 - standard, 145–146
 - risk, 146–147
 - segregation of duties, 146
- Completeness (control objective component), 32
- Completion times (metric), 175
- Compliance/compliance
 - screening, 328–331
 - internal control
 - standard, 329–330
 - regulatory requirements, 329
 - risk, 330–331
- Comprehensive Crime Control Act (1984), 19
- Computer access control, 232–241
 - internal control
 - standard, 234–240
 - risk, 240–241
- Computer controls, 219
 - code of conduct/Tone at the Top, 220
 - internal controls, application, 223
 - metrics, 221–223
 - process, 221
 - sub-processes, 224
- Computer virus, 265
- Conspiracy fraud, 41
- Contingency plan(ning), 255
- Contingent workforce, 149–151
 - internal control standard, 150
 - risk, 151

- Continuous control monitoring (CCM) process, 6, 13
- Contracts
 - administration, 170
 - approvals, cycle time (metric), 191
 - contract-specific requirements, 192
 - defects (metric), 191
 - global/regional contracts, 107
 - renewal/review, 61, 68
 - storage/types, 61
- Control
 - activities
 - ERM component, 30
 - internal control system component, 21
 - deficiency, 27
 - environment (internal control system component), 21
 - objectives, components, 32–33
- Control Objectives for Information and Related Technology (COBIT), 23–24
- Controls self-assessment (CSA), 36–38
 - findings, follow-up/retest, 38
 - IIA definition, 36
 - initiative, scope (determination), 37
 - management reporting/review, 38
 - ongoing training, conducting, 38
 - team, formation, 37
- Cooper, Cynthia, 25
- Copy, 209
- Corporate controls, 15–17
- Corporate credit card, usage, 124
- Corporate frauds (2001–2002), 24–25
- Corporate network, usage, 221
- Corrective action plan, development, 37–38
- Corrective internal controls, 33
- COSO. *See* Committee of Sponsoring Organizations of the Treadway Commission
- Cost accounting procedures/system, 165
- Cost center/management, 213
- Cost of goods sold, 71
- Countback DSO calculation (metric), 52
- Credit, 70
 - availability, 87
 - limits, 62–63
 - validity, metric, 52
 - memos, 74, 118
 - audit trails, 118
 - policies, 62
 - review (internal control standard), 54
 - risk, 64
- Critical controls, 15–17
- CSA. *See* Controls self-assessment
- Customer data validity, 51
- Customer Effort Score (CES), 299
- Customer order cycle time, 155
- Customer order management, 321–324
 - internal control standard, 321–323
 - risk, 323–324
- Customer Satisfaction Rating (CAS), 297
- Customer services
 - internal control, application, 299
 - internal control standard, 300–301
 - metrics, 297, 299

- policy, 300–302
- process, 297
- processes/controls, 298
- risk, 302
- sub-processes, 299
- Customs border patrol (CBP), 111
- Customs brokers, import
 - controls, 112
- D
- Daily cash balances percentage,
 - forecast (contrast), 87
- Data
 - capture, 99
- Days cash available, 87
- Days of Supply (DoS), 156
- Days sales outstanding (DSO),
 - inclusion, 74
- Days sales outstanding (DSO)
 - metric, 52
- Debit balance accounts, 118
- Debit memos, 118
 - audit trails, 118
- Deferred revenue, 69
- Deficiency findings,
 - development, 37
- Delegation of Authority (DoA), 6, 15,
 - 17, 100, 122
 - approvals, 167
- Delinquent DSO calculation
 - (metric), 52
- Delivery metrics, 222
- Depository accounts, 78
- Deposits, cash receipts/application, 77
- Destination Control Statement, 60
- Detective internal controls, 33
- Director, Contracts and Bids
 - North America (DCBNA)
 - compliance, 193
- Disaster recovery, 252–259
 - business process
 - considerations, 253–254
 - internal control
 - standard, 257–258
 - IT business continuity plan,
 - development, 255
 - risk, 258–259
- Disputes/concessions, 64
- Documentation
 - management, 99
 - supporting documentation,
 - 120, 124, 127
- Documented shipments, 65
- Documented supplier
 - selection, 106–107
- Drop shipments, 66, 168
- Duplicate customers, number
 - (metric), 51
- Duties, segregation. *See*
 - Segregation of Duties
- E
- Educational institutions,
 - contracts, 202–203
 - internal control standard, 202
 - risk, 202–203
- Education/training/
 - development, 149
- E-invoicing, 98–99
- Electronic commerce, 261–264
 - definition, 262
 - internal control
 - standard, 262–264
 - risk, 264
- Electronic data interchange
 - (EDI), 261–264
 - definition, 262
 - internal control
 - standard, 262–264
 - risk, 264

- Electronic protection health information (e-PHI), 211
- Employee
 - accounts, 74
 - benefits, 145
 - plans, administration, 146
 - hiring procedures, 147
 - management (H2R process step), 133
 - termination/resignation
 - procedures, 147–148
 - termination/transfer, 138
- End-of-period discounts, usage (limitation), 80
- Endorsements, cash receipts/
 - application, 77
- Enforceable contracts, 61
- Enron, bankruptcy, 24
- Enterprise content management (ECM) systems, 99
- Enterprise-level objectives,
 - establishment/
 - communication, 30–31
- Enterprise Resource Planning (ERP)
 - system, 135
 - implementation/upgrade/
 - consolidation, 6
- Enterprise Risk
 - Management (ERM), 27
 - checklist, 30–31
 - components, 29–30
 - Integrated Framework
 - (2004/2013), 27–35
 - Procure to Pay (P2P)
 - cycle, application
 - (relationship), 28–30
 - systems, 102
- Entertainment, payment process. *See* Payment process
- Entity-level controls,
 - 41–44, 325–339
 - benefits, 42
 - COSO framework, 326
 - evaluation, 43–44
 - internal controls,
 - application, 327–328
 - metrics, 327
 - process, 325
 - sub-processes, 328
- Entity management
 - controls, 334–335
 - internal control
 - standard, 334–335
 - risk, 335
- Entity objectives, achievement, 29
- Environmental controls, 229–232
 - internal control standard,
 - 230–232
 - risk, 233
- Environmental, health, and safety (EH&S), 163
 - compliance, 292
 - internal control, application, 293
 - internal control standard, 294
 - metrics, 293
 - process, 291
 - risk, 295
 - sub-processes, 293
- Environmental, health, safety,
 - and security (EHS&S),
 - 163, 192, 289
- E-payment, 100–101
- E-procurement, 98
- Equal Employment Opportunity
 - compliance, 192
- Equity investments, defining, 85
- Error handling (control objective component), 33

- Established enterprise-level objectives, 30–31
- Ethics, 38–40
 - policy, components, 39
- Event identification (ERM component), 30
- Expense reports, completion, 124
- Export Administration Regulations (EAR), 60
- Export controls, 56–60
 - assessment, 58
 - internal controls, 57–60
 - internal controls standard, 58–60
 - program, elements, 58–59
 - system, government (impact), 56
- External access, 242
- External fraud, 41
- F
- Facilitated team meeting, usage, 36
- Fastow, Andrew, 25
- Feasible contracts, 61
- Federal Acquisitions Regulations (FAR), 192, 197
- Federal Sentencing Guidelines for Organizations (1991), 19–20
- Fill rate, 155
- Financial information
 - accumulation, 180–182
 - internal control standard, 180–181
 - risk, 181–182
- Financial information processing/ reporting, 182–185
 - internal control standard, 182–185
 - risk, 185
- Financial investments, defining, 85
- Financial processes, impact, 329
- Financial reporting, internal control, 31–32
- Financial risk management, 90
- Financial transactions, 174
- Financing operations, 91–92
 - internal control standard, 91–92
 - risk, 92
- Firewalls, 265
- First In, First Out (FIFO), choice, 176
- Fixed assets, 186–188
 - internal control standard, 186–188
 - risk, 188
- Forecast, daily cash balances percentage (contrast), 87
- Forecasted interest expense, accuracy, 87
- Forecasted investment income, accuracy, 87
- Foreign Corrupt Practices Act (FCPA) of 1977, 19, 106, 204
- Foreign currency spot transactions, 94
- Foreign exchange, 94–95
 - hedging, 94–95
 - internal control standard, 94–95
 - risk, 95
 - transactions, 89
- Fraud
 - corporate frauds (2001–2002), 24–25
 - types, 41
- Fraud Triangle concept, examples/ symptoms, 40
- Freeware, 266
- Freight bill accuracy, 155
- Freight claims, 170
- Freight cost per unit, 155

G

General Data Protection Regulation (GDPR), 207, 210–212

General ledger reconciliations, 73, 162–163, 179, 183, 186

Generally Accepted Accounting Principles (GAAP)

IFRS, contrast, 176, 308

usage, 322

General Services Administration (GSA) contracts, sales

identification, 200

Global contracts, 107

Global records

management, 211–212

Global Records Management

Coordinators (GEO-RMC), 212

Global Records Retention Review Committee (GRRRC), 212

Goods receipt — invoice receipt (GR/IR) clearing account

reconciliation, 117

Goods received, acceptance, 114

Government Contract Compliance Plan (GCCP), usage, 193

Government contracts

controls, 190

internal controls, application, 189

metrics, 191

process, 189

sub-processes, 191

Gray market, 302–303

Gross margin return on investment (GMROI), 156

H

Hazardous materials

management, 170

Health Insurance Portability and Accountability Act (HIPAA), 211

Privacy Rule, 211

Health Insurance Portability and Accountability Act Security Rule (HSR), 137–138, 145, 207

Hedging, 94–95

Highly protected risks (HPR)

specifications, 287

Hire to Retire (H2R) process, 133

high-level process steps, 133

internal controls,

application, 136–137

metrics, 135–136

sub-processes, 137

Hiring/termination, 147–148

internal control

standard, 147–148

risk, 148

Human assets, 271

Human Resources (HR), 136

management, 145

payroll automation solutions, 134

planning, 133

policies, 145

responsibilities, 146

Human Resources Glossary, The (Tracey), 136

I

Import controls, 111–113

internal control

standard, 112–113

risk, 113

Information

access, 83

ERM component, 30

- internal control system
 - component, 21
 - Information management, 207
 - internal control,
 - application, 209–210
 - metrics, 209
 - process, 207
 - sub-process, 211
 - systems/tools, 126
 - Information Systems Audit and Control Association (ISACA), 23
 - Information technology (IT)
 - business continuity plan,
 - development, 255
 - policies/operations, 219, 221
 - systems, changes, 248
 - Input controls, 259–260
 - internal control standard, 259
 - risk, 260
 - Institute of Business Ethics, code of
 - conduct, 39–40
 - Institute of Finance & Management (IOFM) survey, 173
 - Institute of Internal Auditors (IIA),
 - CSA definition, 36
 - Institute of Management Accountants (IMA), 20
 - Insurance, 288–290
 - internal control standard, 289
 - risk, 289–290
 - Insurance process, 285
 - insurance/business
 - continuity, 286
 - internal controls, application, 287
 - metrics, 285, 287
 - sub-processes, 287
 - Intellectual assets, 271
 - Intellectual property
 - metric, 273
 - safeguarding, 109, 126
 - Intellectual property,
 - protection, 281–283
 - internal control
 - standard, 281–282
 - risk, 282–283
- Intercompany
 - transactions, 178–180
 - internal control standard, 179
 - risk, 180
- Interdivisional Work Order (IWO),
 - usage, 194
- Interior security, 279–281
 - internal control
 - standard, 279–280
 - risk, 281
- Internal Control — Integrated Framework (1992, 2013), 20–22
- Internal Control — Integrated Framework* (COSO issuance), 29
- Internal controls, 32–33
 - background, 11, 17–27
 - compliance, 105, 174, 190, 208
 - relationship, 102
 - control mechanisms, 33–35
 - corporate controls, 15–17
 - deficiencies, 22
 - effectiveness, factors, 14–15
 - evaluation, 37
 - evaluator roles/responsibilities, 23
 - framework, components, 21
 - fraud prevention, 2–4
 - general standards, 7–8
 - goals/challenges, 11
 - history, 17–27

- key controls, standards
 - (updating), 38
- objectives, 32–33
- risk-based internal controls, 12–14
- system, 14, 21
- systems, monitoring guidance
 - (2009), 32
- toolkit, 1, 5, 8–9
- types, 33–35
- Internal controls, application, 51
 - customer service, 299
 - entity-level controls, 327–328
 - environmental, health, and safety (EH&S), 293
 - export controls, 57–60
 - government contracts, 189
 - Hire to Retire (H2R)
 - process, 136–137
 - procure to pay (P2P) process, 103
 - professional services, 311–312
 - records/information
 - management, 209–210
 - Record to Report (R2R), 177
 - risk-based internal controls, 14–15
 - supply chain, 156
 - Treasury process, 87–88
- Internal controls roles/
 - responsibilities, 44–47, 331
 - internal control
 - standard, 332–333
 - risk, 333
 - standards, 211–213
- Internal control standards (ICS),
 - 5–7, 58–60, 274–277
- accounts receivable (AR), 73–74
- audit committee
 - controls, 336–338
- business continuity, 290
- call center management, 302–303
- compliance/compliance
 - screening, 329–330
- computer access control, 234–240
- credit, 62–64
- customer order
 - management, 321–323
- customer services, 300–301
- development process, 5
- disaster recovery/
 - business contingency
 - planning, 252–259
- educational institutions,
 - contracts, 202
- entity management
 - controls, 334–335
- environmental, health, and safety (EH&S), 294
- financial information
 - accumulation, 180–181
 - financial information processing/
 - reporting, 182–185
- financing operations, 91–92
- fixed assets, 186–188
- implementation/usage,
 - practice, 6–7
- import control, 112–113
- input controls, 259
- insurance, 289
- intellectual property,
 - protection, 281–282
- intercompany transactions, 179
- interior security, 279–280
- internal controls roles/
 - responsibilities, 332–333
- internal record-keeping
 - requirements, 214–215
- international transfer pricing, 178
- inventory control, 159–161
- inventory valuation, 164

- leveraging, 36–38
- market research/product development, 125
- network operations/security controls, 242–244
- non-company networks/bulletin boards, 264–269
- non-U.S. government contracts, 203–205
- opportunity-bid process, 313–314
- order entry/edit, 53–55
- Original equipment manufacturers (OEMs)/Alliance Partners, 167–168
- output controls, 260–261
- paperless transactions/electronic commerce/EDI, 262–264
- payment process, 120–122
- payroll payment controls, 142–143
- payroll preparation/security, 138–140
- perimeter security, 277–278
- physical damage, protection, 288
- physical security/environmental controls, 230–232
- planning/control, 157–158
- premise, 6
- price establishment, 79–80
- procurement cards, 128–130
- product cost management, 165–166
- production restart/recovery, computer/telecommunications backup, 251–252
- professional service, 312–313
- program management, 316–320
- property/casualty risks, 289–290
- purchasing/ordering, 108–110
- revenue recognition/
 - billing, 68–71
 - security framework, 274–276
- state/local government contracts, 202
- supply chain security, 169
- support sales, 308
- systems development methodology, 245–247
- transportation/logistics, 170–172
- Treasury controls, 88–90
- updating, 6, 38
- usage, 5–6
- users/owners/service providers, 226–228
- U.S. government contracts, 193–196
 - commercial products, 199–201
 - non-commercial products, 197–198
 - warranty, 304–307
- Internal environment (ERM component), 29
- Internal fraud, 41
- Internal record-keeping requirements
 - internal control standard, 214–215
 - risk, 215–216
 - standards, 214–216
- International Finance Reporting Standards (IFRS) criteria, 67
- International Financial Reporting Standards (IFRS)
 - GAAP, contrast, 176, 308
 - rules, nonadherence, 338
- International Traffic in Arms Regulations (ITAR), 59–60

- International transfer
 - pricing, 177–178
 - internal control standard, 178
 - risk, 178
 - In-transit inventory, 159–160
 - Intra SoD controls, 101
 - Intrusion Detection System (IDSs), 265–266
 - Invalid customer prices (metric), 51
 - Inventory
 - access safeguards, 160
 - deterioration/damage,
 - protection, 160
 - excess/obsolescence/defects, 161
 - intercompany profit, elimination (information), 161
 - in-transit inventory, 159–160
 - off-site inventory, 160–161
 - receipts/issues, 159, 166
 - recognition, 164
 - records, existence/
 - maintenance, 160
 - supplier-owned consignment
 - inventory, company
 - location, 161
 - turnover, 155
 - Inventory control, 159–162
 - automation solutions, 155
 - internal control
 - standard, 159–161
 - product returns, 160
 - segregation of duties, 159
 - Inventory days of supply, 155
 - Inventory Turnover Ratio (ITR), 156
 - Inventory valuation, 163–164
 - internal control standard, 164
 - risk, 164
 - Inventory velocity (IV), 156
 - Inventory verification, 162–163
 - internal control
 - standard, 162–163
 - risk, 163
 - Investment Advisors Act of 1940, 19
 - Investment Company Act of 1940, 18
 - Investment, policies/transaction/valuation, 93
 - Invoices
 - accuracy/approval, 70, 117
 - delivery, 70
 - e-invoicing, 98–99
 - forwarding, 109
 - scan, 99
 - Isolated environment, 266
 - Item-level standard costs, annual establishment, 165
- K**
- Kerr, Wayne, 42
- L**
- Labor distribution, 165
 - Last In First Out (LIFO), choice, 176
 - Law and public policy (LPP), 327
 - Liability accruals, 118
 - Logic bomb, 266
 - Login requests, 233
 - Low-value requisitions, 110
- M**
- Management
 - commitment, presence, 37
 - directives, 44
 - reporting, 38, 74
 - review, 38, 92

- Marked to market, 95
 - Market research, 125–127
 - internal control
 - standard, 125–127
 - risk, 127
 - Master data (internal control
 - standard), 53
 - Materiality, 180
 - Material/labor transactions, 165
 - Material master data, 158
 - Material weakness, 27
 - Maximum foreseeable loss
 - (MFL), 288
 - Memorandums of Understanding
 - (MOUs), establishment, 194
 - Metrics
 - order to cash process, 51–52
 - Treasury process, 87
 - Missile Technology Control Regime
 - List, dual-use items, 57
 - Monitoring, 21–23
 - COSO monitoring guidance,
 - 22–23
 - elements, 22
 - foundation, establishment, 22
 - internal control system
 - component, 21
 - Monthly closing procedures, 166
 - “Most favored customer pricing,” 80
- N**
- National Association of Purchasing
 - Card Professionals
 - (NAPCP), 127
 - National Institutes of Standards and
 - Technology (NIST), 137
 - Net revenues, 83
 - Network operations, 242–245
 - internal control
 - standard, 242–244
 - risk, 244–245
 - Nickolaisen, Niel, 256
 - “No charge” transactions,
 - recording, 72
 - Non-commercial products/services,
 - development, 197
 - Non-company networks,
 - 264–269
 - internal control
 - standard, 266–268
 - risk, 268–269
 - vulnerability/threat
 - management, 265
 - Non-compliant customer (metric), 51
 - Non-customer payments, 83
 - Non-records, 209
 - Non-standard sales transactions, 68
 - Non-U.S. government
 - contracts, 203–205
 - internal control
 - standard, 203–205
 - risk, 205
 - Non-wage payments, 144
 - Nuclear Regulatory Commission
 - Controls (NRCC), 56
 - Numerically controlled
 - credit memos, 71
- O**
- Objective setting (ERM
 - component), 29–30
 - Office for Civil Rights
 - (OCR), enforcement
 - responsibility, 211
 - Office of Foreign Asset Control
 - (OFAC), 98, 106

- Office of Inspector General (OIG), 98, 106
 - Office of Record, 209
 - Official records, 210
 - Off-site inventory, 160–161
 - “One Face to the Customer” effort, 268
 - Ongoing training, conducting, 38
 - On-time shipping rate, 155
 - Open order review, 54
 - Operating unit, 37
 - Operational Level Agreement (OLA) performance, 223
 - Operations
 - planning, 157
 - Opportunity-bid process, 313–315
 - internal control
 - standard, 313–314
 - risk, 315
 - Oral/side agreements, 61
 - Orders, 53–55
 - access (internal control standard), 53
 - audit trail, 109
 - blanket purchase orders, 109
 - documentation (internal control standard), 54
 - entry/edit, 53–55
 - evidence/fulfillment (internal control standard), 53, 54
 - will-call orders, 71
 - Order to Cash (O2C)
 - automation solutions, 50
 - internal controls, application, 51
 - metrics, 51–52
 - process, 49
 - sub-processes, 53
 - Organization
 - controls, 34–35
 - tone, 38–40
 - Organizational metrics, 222
 - Organization for Economic Cooperation and Development (OECD) Transfer Pricing Guidelines for Multinational Enterprises and Tax Administration, 177–178
 - Organization-level communication, 31
 - Original equipment manufacturers (OEMs)/Alliance Partners, 167–168
 - DoA approval, 167
 - Output controls, 260–261
 - internal control
 - standard, 260–261
 - risk, 261
 - Overhead distribution, 165
 - Owners, 224–229
 - internal control standard, 225–228
 - risk, 225–228
 - Oxley, Michael, 25
- P
- Paperless transactions, 261–264
 - definition, 262
 - internal control
 - standard, 262–264
 - risk, 264
 - Past due customers, 63
 - Payment Card Industry (PCI), 317
 - Payment process, 119–123
 - duties, segregation, 120
 - internal control
 - standard, 120–122
 - risk, 122–123
 - travel & entertainment (T&E), 123–125

- Payments
 - time release, percentage, 87
- Payroll
 - bank accounts, 142
 - checks, security/issuances/
 - distribution, 142–144
 - distribution, 144
 - earnings records,
 - reconciliation, 139
 - expense distribution, 140
 - H2R process step, 133
 - master file, 138
 - procedures, documentation, 139
 - records, 138, 143
 - source data, controls, 139
 - withholdings, 139
- Payroll payment controls, 141–143
 - internal control
 - standard, 142–143
 - segregation of duties, 143
- Payroll preparation/
 - security, 138–141
 - internal control
 - standard, 138–140
 - risk, 140–141
 - segregation of duties, 140
- P-cards. *See* Procurement cards
- Perfect order measurement, 155
- Perimeter security, 276–279
 - internal control
 - standard, 277–278
 - risk, 278–279
- Personal identification, 242
- Petty cash, 122
- Physical assets, 271
- Physical damage,
 - protection, 287–288
 - internal control standard, 288
 - risk, 288
- Physical/electronic
 - records, protection
 - requirements, 217t–218t
- Physical inventory procedures, 162
- Physical safeguards, 33
- Physical security, 229–232, 274
 - control objective component, 33
 - internal control
 - standard, 230–231
 - risk, 232
- Planning/control, 157–159
 - internal control
 - standard, 157–158
 - risk, 158–159
- Point-of-sale (POS) system
 - reports, 303
- Policy controls, 35
- Politically exposed persons
 - (PEPs), 106
- Portfolio credit rating, 87
- Positive pay controls, 121
- PO to invoice conversion, 99
- Preventive internal controls, 33
- Price establishment, 79–81
 - internal control standards, 79–80
 - risk, 81
- Price protection, 69
- Probable Maximum Loss (PML), 288
- Procedure controls, 35
- Process
 - counting procedures, 162
 - metrics, 222
- Procurement cards
 - (P-cards), 127–131
 - audit log, statements
 - tracking, 129
 - internal control
 - standard, 128–130
 - usage, 101

- Procurement cost, 103
- Procurement Integrity Act, 192
- Procure to Pay (P2P)
 - cycle (application), enterprise
 - risk management
 - (relationship), 28–30
 - process, 113
- Procure to Pay (P2P) process, 97
 - accounts payable, 101, 104–105
 - automated matching, 99–100
 - automated workflow approvals, 100
 - data capture, 99
 - document management, 99
 - e-invoicing, 98–99
 - e-payment, 100–101
 - e-procurement, 98
 - functional metrics, 103
 - internal controls, 103, 105
 - invoice scan, 99
 - metrics, 103–105
 - PO to invoice conversion, 99
 - procurement cost, 103–104
 - risk mitigation, automation
 - (usage), 97–102
 - sub-processes, 106
 - supplier portals, 98
- Product
 - cost management, 164–166
 - development, 125–127
 - returns, 68, 109, 160
 - transfers, 65
 - verification, 65
- Production materials, average
 - payment period, 155
- Production restart/recovery,
 - computer/telecommunications
 - backup, 251–252
 - internal control standard, 251–252
 - risk, 252
- Professional services (PS), 309
 - controls, 310, 312–313
 - internal controls,
 - application, 311–312
 - internal control
 - standard, 312–313
 - metrics, 311
 - process, 309
 - risk, 313
 - sub-processes, 312
- Program management, 316–320
 - internal control
 - standard, 316–320
 - risk, 320
- Project Management Institute
 - (PMI), 333
- Promotional activities, 81–84
 - duties, segregation, 83
 - internal control standard,
 - 82–83
 - risk, 84
- Promotion/migration
 - management, 248
- Property/casualty risks,
 - 288–290
 - internal control standard, 289
 - risk, 289–290
- Public companies, guidance, 31–32
- Purchasing/ordering
 - duties, segregation, 108
 - intellectual property,
 - safeguarding, 109
 - internal control standard,
 - 108–110
 - risk, 110–111
- Purchasing strategies, 106
- Q
- Quantity, verification, 65

- R
- Received goods, safeguarding, 115
 - Receiving, 113–116
 - duties, segregation, 114
 - internal control
 - standard, 114–115
 - policy, 114
 - records, changes, 115
 - risk, 115–116
 - Recorded sales transactions, 68
 - Records management,
 - 113, 121, 207
 - classification standards, 208
 - internal control,
 - application, 209–210
 - metrics, 209
 - process, 207
 - sub-process, 211
 - Record to Report (R2R), 173
 - internal controls, application, 177
 - metrics, 175–176
 - process, 175, 182
 - impact, IFRS/GAAP
 - differences, 176
 - sub-processes, 177
 - Recruiting (H2R process step), 133
 - Redeploy (H2R process step), 133
 - Regional contracts, 107
 - Release management, 248
 - Remediation activities,
 - development, 37
 - Remittance inputs, 73
 - Remote access, 233–234
 - Report to the Nations (ACFE), 1
 - Requisitioning procedures, 110
 - Research. *See* Market research
 - Reserves, 68
 - Responsibility (strengthening),
 - qualitative/quantitative targets (impact), 34
 - Retire (H2R process step), 133
 - Revenue
 - reversal, 68
 - types, 69
 - Revenue recognition/billing, 67–72
 - duties, segregation, 69
 - internal control standard, 68–72
 - risk, 71–72
 - Review controls, 35
 - Review error (metric), 175
 - Risk, 55, 61–62
 - appetite, 29
 - financial risk management, 90
 - mitigation, usage, 97–102
 - property/casualty risks, 288–290
 - response (ERM component), 30
 - risk-based internal controls, 12–14
 - Risk assessment
 - ERM component, 30
 - internal control system
 - component, 21
 - Robinson-Patman Act, 80
- S
- SAE 18, 222–223
 - Sales
 - contracts, 60–62
 - cutoff, 66
 - financing, impact, 54
 - goal structure, 80
 - non-standard sales transactions, 68
 - planning, 157
 - process kick-back (metric), 51
 - recorded sales transactions, 68
 - sales weighted DSO calculation, 52
 - terms, 63

- Sarbanes-Oxley 2002 (SOX), 5
 - requirements, 35
 - Section 301, 339
 - Section 404, 6, 12, 28, 31, 44
- Sarbanes, Paul, 25
- Scam, identification, 98
- Scotto, Daniel, 24
- Securities Act of 1933, 18
- Securities Exchange Act of 1934, 18
- Securities, safeguarding, 93
- Security and Exchange Commission (SEC) Acts (1933/1934), 17–18
- Security controls, 242–245
 - internal control
 - standard, 242–244
 - risk, 245
- Security framework, 274–276
 - internal control
 - standard, 274–276
 - risk, 276
- Security metrics, 273
- Segregation of Duties (SoD), 6, 15–16, 128
 - accounts payable, 116
 - accounts receivable (AR), 73
 - cash receipts/application, 77
 - compensation/benefits, 146
 - control, 33, 99, 101
 - credit, 63
 - inventory control, 159
 - payment process, 120
 - payroll distribution, 144
 - payroll payment controls, 142
 - payroll preparation/security, 140
 - promotional activities, 83
 - purchasing/ordering, 108
 - receiving, 114
 - revenue recognition/billing, 69
 - shipping, 66
 - Treasury controls, 88–89
- Self-assessment, approach (steps), 36–38
- Self-audits, 60, 205
- Senior management, commitment/communication, 14
- Service Fulfillment Centers (SFCs), contract placement, 302
- Service Level Agreement (SLA), 248, 317
 - criteria, 150
 - performance, 222
- Service providers, 224–229
 - definition, 225
 - internal control
 - standard, 225–228
 - risk, 228–229
- Shareware, 266
- Shipping, 64–67
 - duties, segregation, 66
 - internal control standard, 65–66
 - partial shipments, 70
 - risk, 66–67
- Single-factor authentication, 234
- Smaller public companies, guidance, 31–32
- SOC 1 Type II Report, provision, 223
- SoD. *See* Segregation of Duties
- Software, 248
- “Special bid” pricing, 80
- Spot transactions, procedures, 94
- SSAE 18
- SSL certificates, configuration (problem), 221

- Standards of internal control. *See* Internal control standards
- State/local government
 - contracts, 202–203
 - internal control standard, 202
 - risk, 202–203
- Statement of Work (SOW), 317
- Statistical sampling, procedures, 162
- Status reporting, 248
- Stockholder information, 92
- Sub-processes
 - asset protection, 274
 - computer controls, 224
 - customer service, 299
 - entity-level controls, 328
 - environmental, health, and safety (EH&S), 293
 - government contracts, 191
 - Hire to Retire (H2R) process, 137
 - insurance process, 287
 - Order to Cash, 53
 - procure to pay (P2P) process, 106
 - professional services, 312
 - records/information management, 211
 - Record to Report (R2R), 177
 - systems controls, 224
 - telecommunications, 224
 - Treasury process, 88
- Supervisory controls, 35
- Supplier
 - discounts, 120
 - operations, 169
 - portals, 98
 - relationships, 126
 - selection, documentation, 106–107
 - statements, 118
- Supplier-owned consignment
 - inventory, company location, 161
- Supplier selection/management, 106–108
 - internal control standard, 106–107
 - risk, 107–108
- Supply chain, 192
 - cycle time, 155
 - inspection, 115
 - internal controls, application, 156
 - inventory control automation, relationship, 154
 - metrics, 155–156
 - planning/control, 157–159
 - process, 153
 - sub-processes, 156–157
- Supply chain security, 169–170
 - contracts/audits, 169
 - internal control standard, 169
 - packaging/palletization, 169
 - risk, 169–170
- Supporting documentation, 120, 124, 127
- Support sales, 307–308
 - internal control standard, 308
 - risk, 308
- Survey approach, usage, 36
- System access, 6, 15–17, 63
 - verification tools, 101
- System owner, 225
- Systems controls, 219
 - code of conduct/Tone at the Top, 220
 - internal controls, application, 223
 - metrics, 221–223
 - sub-processes, 224

- Systems development
 - methodology, 245–248
 - internal control
 - standard, 245–247
 - risk, 247–248
- Systems metrics, 221–222
- SysTrust (1999), 24
- T
- Taxes, 70
- Tax identification number (TIN),
 - validation, 107
- Technology/process gaps,
 - filling, 173, 175
- Telecommunications, 219
 - backup, 251–252
 - code of conduct/Tone at the Top, 220
 - internal controls, application, 223
 - metrics, 221–223
 - process, 221
 - sub-processes, 224
- Terminal/computer
 - identification, 242
- Terminal/computer location, 244
- Third-party accesses, review
 - (frequency), 221
- Threat
 - management, 265
- Time reporting records,
 - approval, 139
- Tone at the top, 14, 38, 42,
 - 174, 190, 208
 - defining, 39
 - problems, examples, 40
- Tracey, William R., 136
- Trade
 - preference programs, 112
 - regulations, 192
- Trade Agreements Act of 1979, 196
- Trading partner, 262
- Trading partner agreement
 - (TPA), 262
- Transportation/logistics, 170–172
 - internal control
 - standard, 170–171
 - risk, 172
- Travel and entertainment
 - (T&E) expenses
 - claims, disbursement, 128
- Travel, payment process. *See*
 - Payment process
- Treasury approvals, 91
- Treasury controls, 88–90
 - duties, segregation, 88–89
 - internal control standards, 88–90
 - risk, 90
- Treasury process, 85
 - code of conduct, 86
 - internal controls,
 - application, 87–88
 - metrics, 87
 - sub-processes, 88
- Trojan horse, 266
- True DSO calculation (metric), 52
- Trustee/issuing, accuracy, 87
- Trust Indenture Act of 1939, 18
- Turn-Earn Index (TEI), 156
- Two-factor authentication, 234, 235
- U
- Unauthorized price changes
 - (metric), 52
- United Nations Security Council
 - (UNSC), resolution 1540, 56
- United States Munitions List
 - (USML), 56
- Users, 224–229

- definition, 225
 - internal control standard, 225–228
 - risk, 228–229
 - U.S. government contracts, 191–197
 - commercial products, 199–201
 - internal control standard, 199–201
 - risk, 201
 - internal control standard, 193–196
 - non-commercial products, 197–199
 - internal control standard, 197–198
 - risk, 198–199
 - risk, 196–197
 - U.S. Sarbanes-Oxley Act of 2002, 25–27
 - best practices, 27
 - requirements, 25–26
- V
- Validity (control objective component), 32
 - Variances
 - analysis/disposition, 166
 - investigation/reporting, 163
 - Vendors
 - performance management, 150
 - selection process, conduct, 108–109
 - Version control, 248
 - Vital business assessment, 256, 257
 - Vital records
 - audit/absence, 258
 - identification, 213
 - maintenance, 212
 - storage, 257
 - Voided/canceled checks, 121
 - Vulnerability, 265
- W
- Warehouse
 - access, 65
 - layout, 65
 - Warranty, 304–307
 - claim threshold, 305
 - internal control standard, 304–307
 - risk, 307
 - Wassenaar Arrangement Dual-Use List, 57
 - Wide Area Network (WAN), 242
 - Will-call orders, 71
 - Wire transfers, 122
 - Work Breakdown Structure (WBS) ID, 317
 - Work team, formation, 37
- Z
- Zero-dollar invoices, 70

<http://www.pbookshop.com>