

---

# Index

---

- absenteeism rates 325–7, 401–4, 425–7
- access controls 43–4, 57–74, 136–7, 242–3, 273–4,  
282–3, 372–5, 380–2, 392–5, 401–7, 453–62,  
481–8, 489–92, 497–501, 504–10, 514–23,  
527–41, 542–53, 555–69, 573–9, 585–9, 613–15,  
620–6, 636–44, 661–6, 667–70, 680–7, 704–6,  
763–834, 842–3  
*see also* data protection...; security
- data protection 620–6, 631–2, 639–44, 848
- data transfers and sharing 515–23, 542–53, 636–44,  
704–6, 850
- freedom of information 479–88, 497–501, 503–10,  
516–23, 525–41, 581–4, 590–1, 627–35, 646–7,  
763–834, 848–9
- hacking 646, 671–9
- human resource information security 661–6, 667–70,  
841–2
- information security incidents 487, 520–3, 671–9,  
841–2
- Internet 599–604, 842–3
- life-cycle issues 661–6
- logging systems 487, 576–9, 588–9, 667–70
- physical security 555–8, 638–44, 661–6, 667–70,  
849
- records management 527–41, 680–7, 849
- remote working 585–9, 844
- rights and responsibilities 661–6
- spreadsheets 704–6
- system access controls 8, 487, 576–9, 661–6, 707–9
- updated access rights 662–6
- user-screening processes 662–6, 667–70, 694–5
- verification tasks 662–6
- access key devices 555–8
- accessibility aspects of information management  
515–23
- accountabilities 33–4, 78, 84, 85–94, 100–15, 282–3,  
448–50, 464–75, 493–5, 535–41, 559–61
- accountancy profession 17
- accounting controls *see* finance and accounting
- accounts payable  
*see also* creditors; purchasing
- concepts 7, 11, 28–9, 33, 42, 45, 51, 240, 246–8,  
436, 713
- control objectives 246
- risk/control questions 246–8
- accounts receivable  
*see also* debtors; order processing
- concepts 7, 33, 42, 240, 248–51, 362, 372–5, 380–2,  
713
- control objectives 248
- risk/control questions 249–51, 362
- accruals 53–60
- accurate information 57–74, 124–7, 242–51, 272–4,  
282–9, 291–316, 493–5, 507–10, 514–23, 535–41,  
559–61, 587–9, 600–4, 618–26, 705–6, 710–11,  
835
- action plans 71–4, 206, 212, 489–92
- activators, systems concepts 131–5
- activities  
categories of organisational activities 6–12
- control activities 117–46, 147–50, 157–8, 164–77
- actuals  
sales performance and monitoring 359–62
- three Es (effectiveness, efficiency, and economy)  
15–16, 19–23, 219–35
- ad hoc internal requests, data transfer types 636, 638–9
- adaptive control systems 133–5
- added value 21–3, 76, 211–12, 219–35, 364–6, 370–1,  
391–2  
*see also* value...
- added value (*cont.*)
- CSAs 211–12
- definitions 22
- operational auditing 21–3, 76, 211–12, 219–35,  
364–6, 370–1, 391–2
- additional voluntary contributions (AVCs) 419
- administrative controls, concepts 3, 6–7, 117
- advertising *see* promotion and advertising
- affiliates 158, 177
- Afghanistan 729, 764
- after sales support 5–6, 8, 43, 126–7, 343–4, 348, 350,  
366, 375–82, 389–92, 714–15, 724  
*see also* maintenance and servicing; marketing and  
sales; spare parts...; warranty arrangements
- concepts 8, 343–4, 375–82, 389–92, 714–15, 724
- control objectives 375–6, 377–8, 380–1, 389
- risk/control questions 376–7, 378–80, 381–2,  
389–92

- after sales support (*cont.*)
- SAPG 714–15, 724
- agents 8, 343, 350, 351–3, 362, 368–71, 404–7, 714
- concepts 350, 351–3, 362, 368–71
  - conflicts of interest 369–71
  - control objectives 368–9
  - remuneration 368–71
  - responsibilities 369–71
  - risk/control questions 369–71
- AGMs 93
- AICPA 116–18
- air conditioning systems, systems concepts 130–5
- Albania 729, 764
- allowances, taxation 264–6
- annual reports 92–4, 117, 151–77, 251–3, 710–11
- see also* Sarbanes-Oxley Act 2002
- anonymous voting systems 205, 207–8
- anti-discrimination laws 406–7, 594–5
- appendices 616, 712–851
- Apple Corporation 570–1
- appointments, auditors 17, 176
- approval issues
- boards of directors 17, 73–4, 164, 166, 211
  - lists of contractors 9, 290, 297–9, 316
- archives 514–23, 538–41, 680–7, 835
- Argentina 730, 765
- Armenia 730, 765
- ARPANET 598
- Ashby's cybernetics law of requisite variety 131–5
- asset management 481–8, 710–11
- asset registers 497, 502–10, 515–23, 527–41, 556–8, 681–7, 700–1, 710–11, 847, 850
- assets
- see also* hardware...; information...; software...
  - fixed assets (and capital charges) 7, 240, 253–6, 432–6, 447, 502, 710–11
  - risk management 3, 5–6, 10, 17, 22, 25, 29–30, 36–7, 40, 41–74, 76–94, 95–115, 143–5
- assurance issues 8, 17–19, 22, 75, 82–4, 100, 115, 117–46, 171–3, 182–7, 212, 214–35, 240–75, 286–9, 306–10, 314–16, 318, 319–42, 345–81, 468–75, 714, 721
- see also* quality assurance...
  - boards of directors 82–4
  - resourcing decisions 17–19, 232–5
- ATMs 10
- attachments, emails 593–7, 691–3
- audit approaches to operational auditing 12–16
- audit committees 32–3, 82–4, 86–7, 88–90, 114, 127–8, 143–5, 153–77, 211–12, 214–35
- see also* boards of directors
  - chief audit executives 82–4, 143–5, 232–3
  - complaints 160
  - CSAs 211–12
  - financial experts 158–62, 172–3
  - monitoring functions 127–8, 143–5, 158–77
  - responsibilities 158–73, 176–7, 211, 214–35
  - Sarbanes-Oxley Act 2002 153–77
  - statutory requirements 158–60
- audit findings 13–14
- audit logs *see* logging systems
- audit reports 13–14, 200–1, 218, 226–35
- audit review programmes, joint ventures 283
- audit trails, concepts 35, 36, 168–70, 247–8
- audit universes
- business processes 27–39, 41, 240
  - concepts 6, 9, 11, 27–39, 41, 290
  - contracting 9, 290
  - hybrid audit universe 30
- audit visits 45, 277–84
- auditors
- appointments 17, 176
  - credibility issues 11–12, 16–18
  - knowledge/skills/competencies requirements 16–18, 86–7, 158–60, 218, 233–4
  - recruitment issues 17, 176
  - remuneration 176, 233
  - technical activities 16–19
- Australia 534, 581, 635, 730, 765–6
- Austria 731, 767
- authority to make organisational commitments 136–7, 147–50, 183–5, 203–4, 208–13, 550–3, 554–8
- automated controls 130–5, 195–8
- back-up and media management 8, 43–4, 67–74, 486, 497–501, 505–10, 521–3, 537–41, 558, 562–5, 584, 658–60, 846
- concepts 562–5, 584, 588–9, 846
  - control objectives 563
  - procedures 563–5, 846
  - risk/control questions 563–5
- BACS 245, 261, 487, 696–8
- bad debts 33, 249–51
- BAE 97–8
- balance sheets 54, 67–74
- bank account reconciliations 258–61
- bank accounts and banking arrangements
- concepts 7, 240, 258–61, 283, 713
  - control objectives 258–9
  - risk/control questions 259–61
- banks 29, 42, 51, 97–8, 283
- Barbados 731, 768–9
- batch processing 559–61
- Belarus 731, 769
- Belgium 732, 770
- benchmarking, concepts 16, 23–4, 92, 172–3, 349–50, 354
- Bermuda 732–3, 770–1
- BERR 481, 585, 590–1, 599, 658, 671–2, 691, 851
- 'best' row in control matrices 58–74
- bibliography 852–7
- Blair, Tony 151
- boards of directors 4–5, 9–10, 12–14, 17, 32, 44, 73–4, 75–94, 102–8, 112–15, 117–46, 147–50, 153–77, 211–12, 215–35, 470, 524–41, 552–3
- see also* audit committees
  - approval requirements 17, 73–4, 164, 166, 211
  - assurance vacuums 82–4

- committees 32–3, 82–4, 86–7, 88–90, 93, 114  
 corporate governance 81–94, 176–7, 470  
 CSAs 211–12  
 direction-setting objectives 81–2, 87–8, 147–50  
 internal controls 117–46, 151–77, 470  
 objectives 81–4, 87–90, 112–15, 117–46, 147–50, 176–7, 470, 552–3  
 organisational objectives 81–2, 87–90, 112–15  
 risk management 102–8, 112–15, 470  
 risk registers 107–8, 115  
 bomb threats 556–8  
 Bosnia and Herzegovina 733, 771–2  
 ‘both’ row in control matrices 58–74  
 Botswana 733, 772–3  
 bottom-round management, concepts 196–8  
 bought-in expertise, technical activities 17–18  
 boundaries, systems concepts 131–5  
 BPR *see* business process re-engineering  
 brainstorming sessions 57, 106–7, 183, 207–8  
 Brazil 733, 774  
 break-even points 269–70  
 breakdown services, company vehicles 435–6  
 bribery 84–5  
 British Petroleum (BP) 17–18, 199  
 British Security Industry Association (BSIA) 684  
 British Standards Institute (BSI) 182, 183–4, 466–7, 480–8, 526  
   *see also* ISO...  
   background information 182, 183–4, 466–7, 480, 526  
   BS 4783 526  
   BS 5454 526  
   BS 7499 555  
   BS 7750 467  
   BS 7799 480–1, 526  
   BS 8555 466–7, 475  
   BS 15000 483  
   BS EN 15713 684  
   DISC PD0010 526  
   DISC PD0012 526  
 ‘budget/actual comparisons’, operational auditing  
   evaluations 223–33  
 budgeting and monitoring 7, 51, 71–4, 223–35, 240, 256–8, 268–70, 276–84, 287–9, 293–316, 351–3, 388–92, 406–7, 413–15, 442–5, 490–2, 652–4, 710–11, 713  
   control objectives 256, 443–5  
   IT accounting 710–11  
   risk/control questions 257–8, 443–5  
 buildings  
   IT sites and infrastructure 555–8, 658–60, 681–7, 843  
   portable buildings 111  
 builds of software, concepts 571–5  
 Bulgaria 734, 774–5  
 business continuity plans (BCPs) 497–501, 521–3, 846–7  
   *see also* contingency plans  
 business cycles, concepts 32–5, 240  
 business management techniques  
   *see also* delaying...; empowerment...;  
   outsourcing...; quality assurance... concepts  
   178–98  
   JIT 178, 195–8  
 business plans 282–3  
 business process re-engineering (BPR), concepts  
   178–81, 188–90, 199  
 business processes  
   concepts 3–4, 27–39, 41, 116–46, 167–73, 178–81, 199–213, 240, 712–28, 837  
   contracting 32  
   CSAs 30, 199–213  
   definitions 32–5, 837  
   hallmarks of robust business processes 36, 141–2, 507–10, 521–3, 587–9  
   identification approaches 32–5  
   lists 32–5  
   SAPGs 35–6, 712–28  
   Sarbanes-Oxley Act 2002 167–73  
   university case study 37–9  
   weaknesses 30–2  
 Cadbury, Sir Adrian 116  
 CAE 13, 18  
 ‘calculated risk score’ row in control matrices 58–74  
 campus area networks (CANs) 609  
 Canada 117, 129–30, 154, 199, 685, 734–7, 775–81  
   *see also* CoCo  
 capacity management 486, 497, 511–13, 520–3, 715, 725, 846  
   control objectives 512  
   definition 511–12  
   risk/control questions 512–13  
 Cape Verde 737–8, 781  
 capital expenditure, hardware assets 502, 713, 721  
 carbon trading 464–5  
 cash 7, 11, 32–6, 42, 54, 135–6, 240, 245–6, 258–61, 270–2, 274–5, 720–8  
   *see also* petty cash...  
 cash flow management 33–4  
 Cayman Islands 738, 781–2  
 CCTV 554–5, 673  
 CDs 497, 533, 566–7, 637, 672  
 CEOs 97–8, 117, 128–9, 163–77, 229, 232–3  
 CERN 598  
 certification requirements  
   CSAs 200  
   Sarbanes-Oxley Act 2002 151–77  
 Certified Internal Auditors (CIAs) 204  
 CFOs 117, 128–9, 163–77  
 change management 497–501, 506–7, 520–3, 547–53, 605–8, 845–6  
 CHAPS 261  
 Chartered Institute of Public Finance and Accountancy (CIPFA) 228–30  
 Charters, operational auditing 217–35  
 cheques 259–61  
 chief accountants 4, 58, 69, 164–77

- chief audit executives 18–19, 82–4, 143–5, 171, 216–35, 470
- audit committees 82–4, 143–5, 232–3
- ‘for pay and rations’ reports 83–4
- resourcing considerations 18–19, 232–3
- Chile 738, 782
- China 581, 739, 782–3
- CIAAs *see* Certified Internal Auditors
- CIPFA *see* Chartered Institute of Public Finance and Accountancy
- classifications of organisational activities, concepts 6–12
- cleaning firms, outsourcing considerations 192, 193
- ‘clear desk’ policies 539–40, 840–1
- clearing banks 29
- clients 13–14, 222–35
- see also* customer...
- closed systems, concepts 131–5
- CoCo internal control framework 117–18, 129–30, 141–3, 144, 157–8, 208–10
- see also* Canada
- Codes of Conduct, ethics 148–9, 161–3, 172, 215–35
- collection aspects
- data protection 618–26
- information asset registers 505–6, 847
- information management 515–23, 542–53, 618–26
- collusion, fraud 149–50
- colour codes and numeric scores, risk matrices 104–6
- comfort letters 164
- commitment factors 136–7, 147–50, 183–5, 203–4, 208–13, 550–3, 554–8
- Committee of Sponsoring Organizations (COSO) 4–5, 15, 75–81, 96–9, 103, 111, 115, 117–28, 140, 142, 144, 147–50, 157–77
- Common Law Duty of Confidence 640
- communications 17–18, 20, 28–9, 78, 81–4, 85–7, 89–94, 99–115, 120–1, 124–7, 196–8, 208–13, 234, 277–84, 366–8, 430–2, 427, 489–92, 497, 515–23, 542–53, 554–8, 581–4, 590–7, 840
- emails 487, 497, 520–3, 581–4, 590–7, 691–3, 841
- JIT coordination 196–8
- knowledge management 542–53
- labour relations 430–2
- sharing aspects of information management 515–23, 542–53, 636–44
- subsidiaries/joint ventures 277–84, 366–8
- Communities of Practice (CoPs) 547
- Companies Act 2006 464, 473–5
- company vehicles 7, 399, 432–6, 556–8, 714
- control objectives 433
- risk/control questions 433–6
- comparators, systems concepts 130–5
- competencies 9, 16–18, 84–5, 122, 129–30, 147–50, 158–77, 208–13, 290, 295–7
- competitive advantages 71–4, 279–80, 344–55, 362–6, 368–9, 388–92, 411–13, 468–75, 489–92
- competitive disadvantages 57–74
- complaints 126–7, 160, 350, 356–7, 362, 406–7
- completeness of information flows 14, 124–7, 168–73, 272–4, 283–9, 291–316, 507–10, 515–23, 535–41, 559–61, 587–9, 705–6, 710–11, 835
- compliance issues 4–5, 46–50, 55, 60–74, 77–94, 96–115, 117–46, 151–77, 202, 226–35, 242–75, 291–316, 319–42, 400–36, 439–52, 463–75, 479–88, 496–501, 514–41, 616–35, 640–4, 665–6, 707–11, 713–14, 721, 835
- see also* legislation; regulations
- ‘compliance testing’ column of SAPG risk/control section 48–50
- Computer Misuse Act 1990 581, 646
- concealed risks 107–10
- confidentiality 57–74, 124–7, 220–1, 242–3, 272–4, 299–302, 345–8, 351–5, 401–7, 438–42, 453–62, 503–10, 515–23, 533–41, 560–1, 566–9, 586–9, 592–7, 637–44, 663–6, 671–9, 680–7, 688–90, 700–6, 729–62
- configuration management database (CMDB) 572
- conflicts of interest
- agents 369–71
- distributors 362–6, 389–92
- ethics 162–4
- consistency of information flows 14, 124–7, 272–4, 705–6
- consulting roles 100, 115, 180–1, 212, 232, 542
- contingency plans 43–4, 69–74, 91, 103, 368, 397–8, 453–62, 487, 497–501, 512–13, 528–41, 561, 658–60, 671–9, 689–90, 707–9, 846–7
- see also* business continuity plans
- concepts 658–60, 689–90
- control objectives 658–9
- risk/control questions 659–60
- security 453–62, 528–41, 658–60
- subsidiaries 368
- tests 658–60, 689–90
- continuous improvements 16, 77–80, 91–4, 140–1, 179–81, 182–7, 210–13, 315–16, 466–7
- see also* total quality management
- contract management environment
- concepts 9, 290–5
- control objectives 291–2
- risk/control questions 292–5
- contracting 6, 7, 9, 22–3, 32, 44, 143–5, 191–5, 220–1, 234, 285, 289–316, 385–92, 648–50, 655–7, 683–7, 716–17, 727–8
- see also* outsourcing...; procurement; tendering
- approved lists of contractors 9, 290, 297–9, 316
- audit universes 9, 290
- business processes 32
- concepts 285, 385–92, 648–50, 655–7, 683–7, 716–17, 727–8
- control objectives 291–316, 388–9, 655
- costs and benefits analysis 291–316, 648–50, 655–7
- definition 289–90
- disposal of records 683–7
- documentation 300–1, 302–10, 314–16
- final accounts 9, 290, 310–13
- insurance cover 296, 389–92

- interim payments 9, 44, 290, 308–13
- overview of audit universes 9, 290
- performance/productivity measurement systems 9, 290, 306–8, 313–16, 385–92
- reviews of project outturn/performance 313–16
- risk/control questions 292–316, 649–50, 656–7
- SAPG 716–17, 727–8
- selection and letting issues 9, 290, 304–6
- viability/competence assessments of contractors 9, 290, 295–7
- contracts of employment 405–7, 441–2
- control activities
  - concepts 117–46, 147–50, 157–8, 164–77, 207–13, 281–4, 707–9
  - dimensions 123–4
  - joint ventures 281–4
  - ‘control activities’ component, COSO internal control framework 120–1, 123–4, 142, 144, 147–50, 157–8, 164–77
  - ‘control environment’ component, COSO internal control framework 120–2, 147–50, 157–77
  - control environments 120–2, 147–50, 152–77, 453–5, 712–13, 721
  - control matrices
    - see also* inherent risk
    - concepts 40, 53–4, 56–74
    - examples 56–74
    - MISs 56–74
    - planning 64, 71–4
  - control registers, Sarbanes-Oxley Act 2002 168–70, 173
  - control self assessments (CSAs)
    - see also* standard audit programme guides
    - action plans 206, 212
    - anonymous voting systems 205, 207–8
    - audit committees 211–12
    - business processes 30, 199–213
    - CoCo internal control framework 208–10
    - concepts 18–19, 30, 41, 102–3, 128, 199–213, 718
    - control objectives 210–12
    - costs and benefits analysis 202–4, 205–6, 211–12
    - critique 205–6
    - definition 18–19, 41, 199–200
    - hybrid approaches 206–7
    - IIA CCSA programme 204, 210
    - management commitment needs 202–3
    - negative perspectives 202–3
    - origins 199
    - questions 208–12
    - readings 210
    - reassurance aspects 206
    - responsibilities 200–2
    - suitable focus areas 200–1
    - top-down commitment 203–4
    - training 204–5, 212
    - Word tables 206
    - workshop/survey approaches 200–1, 204–12
  - control systems, concepts 130–5
  - control-effectiveness measurements 54–6, 57–74, 78, 84, 85, 127–8, 141–3, 151–77, 209–13, 219–35
  - control-risk self assessments *see* control self assessments
  - controls, concepts 116–46
  - conversion business process, concepts 720–8
  - Coopers & Lybrand 118
  - coordinated sections within businesses 3–26, 27–39, 78–94, 116, 118–20, 196–8, 200–1, 218
  - Copyright Designs and Patents Act 1988 581, 646
  - core/non-core activities, outsourcing considerations 193–4, 195
  - corporate framework business process, concepts 34–5, 720–8
  - corporate governance 3, 5–6, 9–10, 17, 22, 25–6, 29–30, 34, 44, 75–94, 176–7, 205, 232–5, 470–5, 509–10, 718, 836
    - best practices 93, 228–30
    - boards of directors 81–94, 176–7, 470
    - communications 78, 81–4, 85–7, 89–94
    - concepts 75–94, 175–7, 205, 470–5, 509–10, 718, 836
    - external governance processes 75, 81–4, 90–4, 116
    - internal controls 76–94
    - internal governance processes 78, 81–2, 84–7
    - international conflicts of standards 176–7
    - objectives 77–94
    - risk management 76–94, 110
    - SAPG 718
    - stakeholders 75–82, 90–4
  - corporate memory, concepts 545–53
  - corporate social responsibilities 16, 21, 91–4, 463–75
  - corrective category of control 139, 168–70
  - corrective control systems 135
  - corrupted data 57–74
  - COSO *see* Committee of Sponsoring Organizations
  - costing methods 268–70, 321, 345–8, 354–5, 438–42, 445–50, 710–11, 720–8
  - costs and benefits analyses 151, 154–5, 171–2, 183–5, 188–9, 192–4, 197–8, 202–4, 205–6, 211–12, 219–35, 286–9, 291–316, 327–30, 349–50, 360–2, 411–13, 442–5, 460–2, 466–75, 507–10, 648–50, 651–7
    - see also* budget. . .
  - CRB *see* Criminal Records Bureau
  - credibility issues, auditors 11–12, 16–18
  - credit cards 272
  - credit notes 249–51
  - credit-granting business process 32–3, 136, 138, 194, 249–51, 371–5
    - see also* order processing
  - creditors 33–4, 91–4, 242–3, 246–8
    - see also* accounts payable
  - creditworthiness appraisals 249–51
  - Criminal Justice and Public Order Act 1994 617
  - Criminal Records Bureau (CRB) 663, 665–6, 841–2
  - criminal sanctions
    - data protection 617–18, 625–6
    - Sarbanes-Oxley Act 2002 152–4, 164–77

- crisis response plans 91, 494–5, 497–501, 536–41, 556–8, 658–60, 671–9, 707–9, 842, 847
- Croatia 740, 784
- CSAs *see* control self assessments
- cultural issues 29–30, 34, 57–8, 85–6, 110, 115, 121–2, 183–7, 220–1, 277–84, 496–501, 532–41, 547–53, 598, 678–9, 840
- JIT 196
- joint ventures 280–1
- knowledge management 547–53, 849–50
- outsourcing considerations 192, 193, 220–1
- quality assurance systems 183–7
- subsidiaries 277–84, 366–8
- ‘current control/measure’ column of SAPG risk/control section 48–50
- customer-focused marketing 344, 348–50, 356–9, 369
- customers 91–4, 126–7, 180–1, 222–5, 344–82
- after sales support 5–6, 8, 43, 126–7, 343–4, 348, 350, 366, 375–82
- complaints 126–7, 350, 356–7, 362
- credit-granting business process 32–3, 136, 138, 194, 249–51, 371–5
- requirements 344–50, 388–92
- Customs and Excise (C&E) 262–3, 622
- cybernetics 130–5
- cycles
- concepts 27–39, 372–5, 468–75, 544–5, 547–9, 661–6, 680–7
- definition 32
- university case study 37–9
- Cyprus 740, 784–5
- Czech Republic 740, 785
- damage or distress to data subjects situations, data protection 617, 620, 625, 835
- data controllers, data protection 617–26, 729–62, 835
- data definitions 542–5, 835–6
- see also* knowledge...
- data protection 9, 43–4, 404–7, 479–88, 496–501, 503–10, 514–23, 525–41, 562–5, 581–4, 590–7, 616–26, 631–2, 639–44, 646–7, 700–6, 729–62, 835, 842, 848
- see also* access...; sensitive...
- access requests 619–26
- concepts 479–88, 514–23, 525–41, 581–4, 590–1, 616–26, 631–2, 639–44, 646–7, 700–6, 729–62, 835, 842, 848
- control objectives 625
- criminal sanctions 617–18, 625–6
- damage or distress to data subjects situations 617, 620, 625, 835
- errors 617, 620, 625, 626, 848
- exemptions 621, 624
- international legislation 616, 729–62, 848
- objectives 617
- principles 618–26, 631–2, 639–41, 848
- processes 619–26
- risk/control questions 625–6
- time limits 620, 625
- Data Protection Act 1998 616–26, 639–44, 646, 759–60, 835, 838, 842, 848
- data retention and disposal 487, 497, 524–41, 562–5, 620–6, 638–44, 680–7, 836, 851
- see also* disposal...; retention...
- concepts 680–7, 836, 851
- control objectives 685
- life-cycle issues 680–7
- risk/control questions 685–7
- standards 684–5
- data subjects, data protection 617–26, 642, 729–62, 835
- data transfers and sharing 487, 497, 515–23, 542–53, 636–44, 688–90, 704–6, 850
- ad hoc internal requests 636, 638–9
- concepts 636–44, 688–90, 704–6, 850
- control objectives 642, 688–9
- exemptions/exceptions 637–8
- ISAs 639–44
- regular transfers with external parties 636–7, 639–44
- risk/control question: 643–4, 689–90
- types 636–8
- databases 9, 42, 57–74, 136–7, 487, 502–10, 544–53, 613–15
- see also* information asset registers
- concepts 613–15
- control objectives 613–15
- risk/control questions 614–15
- debt collectors 194
- debtors 33, 194, 248–51, 371–5, 378–82
- see also* accounts receivable; order processing
- delaying considerations, concepts 178, 187–9
- Denmark 740, 785
- depreciation 253–6, 434–6
- detailed issues, SAPG questions 46–50
- detective category of control 138–9, 144, 168–70
- detectors, systems concepts 130–5
- developing world, environmental issues 465–6
- development project management 8, 437, 447–50, 715
- control objectives 447–8
- definition 447
- risk/control questions 448–50
- digital cameras 567
- digital preservation
- concepts 531, 532–41, 681–7
- definition 532
- direct marketing, data protection 620
- directive category of control 138
- directors 4–5, 9–14, 17, 32, 44, 73–4, 75–94, 102–3, 107–8, 112–15, 117–46, 147–50, 153–77, 211–12, 215–35, 464, 470, 524–41
- see also* boards...
- disaster recovery plans (DRPs) 91, 494–5, 497–501, 536–41, 556–8, 563–5, 574–5, 658–60, 671–9, 707–9, 842, 847
- disciplinary/grievance procedures 7, 85, 149, 399, 400–4, 424–7, 594–7, 604, 641–4
- concepts 424–7, 594–7, 604
- control objectives 425
- risk/control questions 425–7, 597, 604



- disclosures
  - information management 515–23
  - Sarbanes-Oxley Act 2002 151–77
- discount policies *see* pricing and discount policies
- discussion boards 600–4
- disposals 433–6, 447, 487, 497, 505–6, 514–23, 524–41, 562–5, 620–6, 638–44, 680–7, 836, 851
  - company vehicles 433–6
  - control objectives 685
  - information asset registers 505–6, 515–23, 681–7
  - R&D equipment 447
  - records management 527–41, 680–7, 849, 851
  - removable media 567–9
  - resurrected deleted files 562, 567, 682–7, 851
  - risk/control questions 685–7
  - standards 684–5
- dissemination *see* sharing...
- distribution
  - see also* logistics; stock...; transport; warehousing...
  - concepts 7–8, 383–98, 714
  - control objectives 384–98
  - insurance cover 385–98
  - operational auditing 7–8, 383–98
  - overview 383–4
  - risk/control questions 384–98
- distributors 3, 8, 33, 35, 42–3, 343, 362–6, 382, 383, 388–92, 714
  - concepts 362–6, 382, 383, 388–92
  - conflicts of interest 362–6, 389–92
  - control objectives 362–3, 388–9
  - definition 362, 388
  - performance/productivity measurement systems 362–6, 388–92
  - risk/control questions 363–6, 389–92
- diversity issues 16, 21, 84–5, 93, 406–7, 594–7
  - see also* anti-discrimination...; equal opportunity...; equity... boards of directors... 93
  - three Es of equity, environment, and ethics, concepts 16, 21, 84–5, 93
- division-with-supervision opportunities, internal controls 135–7, 142–3, 150
- documentation 36–7, 40–74, 167–73, 182–7, 197–8, 218, 241–3, 262–3, 272–5, 286–9, 291–316, 335–42, 375–82, 411–13, 443–5, 494–5, 535–41, 544–53, 606–8, 652–4, 681–7, 695, 701–6, 712–28, 839–51
  - see also* standard audit programme guides
- drivers, definition 571
- Drucker, P.F. 111
- due diligence 87–8
- DVDs 497, 566–7, 637
- Eastern Europe 280–1
- economy issues
  - concepts 4, 15–16, 19–23, 29–30, 77–9, 219–35, 319–42
  - performance/productivity measurement systems 19–23, 219–35, 319–42
- three Es (effectiveness, efficiency, and economy) 15–16, 19–23, 29–30, 219–35
- EDI *see* electronic data interchange
- EDMS *see* electronic document management systems
- 'effective yes/no' column of SAPG risk/control section 48–50
- effectiveness issues
  - concepts 4–5, 15–16, 19–23, 29–30, 54–6, 76, 78, 84, 85, 88–9, 95–115, 117–46, 209–13, 219–35, 313–16, 319–42, 352–3, 557–8, 612
  - control-effectiveness measurements 54–6, 78, 84, 85, 127–8, 141–3, 151–77, 209–13, 219–35
  - corporate governance 78, 84, 85, 88–9
  - performance/productivity measurement systems 19–23, 78, 84, 85, 219–35, 313–16, 319–42
  - three Es (effectiveness, efficiency, and economy) 15–16, 19–23, 29–30, 117–46, 215–35
- efficiency issues
  - concepts 4–5, 15–16, 19–23, 29–30, 77–9, 95–115, 117–46, 215–35, 319–42, 595–7
  - performance/productivity measurement systems 19–23, 219–35, 319–42
  - personnel 15–16
  - three Es (effectiveness, efficiency, and economy) 15–16, 19–23, 29–30, 117–46, 215–35
- Electronic Communications Act 2000 581, 646
- electronic data interchange (EDI) 43–4, 198, 248–50, 487, 688–90
  - control objectives 688–9
  - risk/control questions 689–90
- electronic document management systems (EDMS) 531
- electronic funds transfers 242–5, 259–61, 487, 696–8
- electronic records, types of records 496–7, 502–3, 524–41, 545–53, 566–9, 622–6, 631–2, 681–2, 712–28
- emails 487, 497, 520–3, 581–4, 590–7, 646, 691–3, 841
  - see also* information technology
  - attachments 593–7, 691–3
  - concepts 590–7, 691–3, 841
  - control objectives 595–6
  - policies 591–7, 841
  - Regulation of Investigatory Powers Act 2000 581, 592, 646
  - risk/control questions 596–7
  - spam 590–7, 602, 707–9
  - standard formats 593–7
  - statistics 590–1
  - viruses 691–3, 841
- embedded microchips 567
- emergency/evacuation drills 428–30, 455–62, 556–8
  - see also* disaster...
- empowerment considerations, concepts 178, 188, 189–91, 195–6, 211–12
- encrypted data 566–9, 610–12, 638–44, 646, 673, 845
- energy *see* materials and energy
- Enterprise Risk Management framework (COSO) 75–6, 96–115, 119, 120–1, 140, 157–8
- environmental auditing, concepts 465–75

- Environmental Information Regulations 2004 526, 646
- environmental issues 8, 16, 41, 42–3, 219–35, 318,  
335–8, 463–75, 713–14, 721  
assessments 468–9  
control objectives 335–6, 465, 471  
developing world 465–6  
EMAS 464, 466–70, 475  
emergence of concerns 465–6  
example programmes 470–5  
experts 469–70  
hazardous materials 332–8, 395–8, 428–30, 457–60,  
463–75, 554–8  
legislation 463–75  
physical security 332–5, 428–30, 454–62, 495,  
496–501, 520–3, 554–8, 588–9, 638–44, 849  
production/manufacturing 8, 318, 335–8  
responsibilities 463–75  
risk/control questions 336–8, 465, 471–5  
strategic objectives 467–8  
supply chains 468–75  
sustainability reports 470–5  
systems concepts 131–5  
three Es of equity, environment, and ethics 16, 21,  
84–5, 463–75  
waste management 335–8
- equal opportunity laws 406–7
- equity issues  
*see also* diversity...  
three Es of equity, environment, and ethics 16, 21,  
84–5
- errors  
data protection 617, 620, 625, 626  
keying errors 57–74, 699–700  
spreadsheets 699–700, 702
- estates management 430, 712–13
- estimates 158–60
- Estonia 741, 786–7
- ethics 16, 34, 78, 84–5, 121–2, 147–50, 161–3, 172–3,  
209–13, 215–35, 288–9, 415–22, 437, 464–75,  
594–7  
Codes of Conduct 148–9, 161–3, 172, 215–35  
conflicts of interest 162–4  
environmental issues 464–75  
management 147–50, 161–3, 172–3, 209–13  
pension schemes 415–22  
questions 147–50, 172  
research and development 437  
Sarbanes-Oxley Act 2002 161–3, 172
- Ethiopia 742, 787
- Europe  
*see also individual countries*  
contracts 300  
data protection legislation 729, 742  
digital preservation 535  
freedom of information 627–8, 763
- European Commission's Eco-Management and Audit  
Scheme (EMAS) 464, 466–70, 475
- European Convention on Human Rights (ECHR) 628,  
763
- European Economic Area 621–6
- European Union Directive on Data Protection (95/46/EU)  
742
- Excel 702–4  
*see also* spreadsheets
- exemptions from VAT 263
- expenditure business process, concepts 33–4, 36, 720–8
- expenses 7, 11, 240, 270–2, 356–9, 433–6  
control objectives 271, 356–9  
petty cash and expenses 7, 240, 270–2  
risk/control questions 271–2, 356–9
- expert systems 9, 44
- experts  
environmental issues 469–70  
research and development 437–52
- external auditors 151–77
- external governance processes, concepts 75, 81–4,  
90–4, 116
- external hard drives 566–7
- external reviews, operational auditing 214, 216–17
- extranets 610
- facilitation roles, operational auditing 201–6, 212
- facilities management (FM) 9, 43–4, 192, 487, 648–50,  
655–7  
*see also* information technology; outsourcing...  
concepts 192, 648–50  
control objectives 648–9  
definition 192, 648  
risk/control questions 649–50
- facilities, plant and equipment  
*see also* maintenance  
concepts 8, 318, 319–24, 339–42, 427–30, 445–7,  
457–60, 486, 554–8, 714  
R&D equipment 8, 437, 445–7
- fact-finding programmes 45, 277–8
- failures 91, 141–3, 151–77, 315–16, 317–42, 375–82,  
494–5, 497–501, 512–13, 523, 536–41, 556–8,  
563–5, 574–5, 658–60, 671–9, 699–700, 707–9
- Fayol, Henri 116, 118, 187–8, 198
- feed system direct interfaces 57–74
- feedback systems 130–5, 234, 350, 356–7, 362, 545–53
- feedforward, systems concepts 132–5
- fees 158–60, 164–77
- FEI surveys 155
- Fiji 742, 787–8
- file headers 68–74
- final accounts for contractors 9, 290, 310–13
- finance and accounting  
accounting policies 710–11  
concepts 3, 6, 7, 27, 32–5, 42, 117, 143–5, 192,  
197–8, 239–75, 710–11, 713, 722  
control objectives 240–75  
cyclical definition 240  
definition 117, 239–40  
functional definition 240  
IT accounting 710–11  
JIT 197–8  
management 239–75



- overview of functions 7, 240
- risk/control questions 240–75
- SAPG 713, 722
- system/function components 239–40
- finance directors 4
- financial controls 3, 143–5
- financial experts, audit committees 158–62, 172–3
- financial information and reporting
  - concepts 7, 240, 272–4, 710–11, 713
  - control objectives 272–3
  - risk/control questions 273–4
  - standards 272–4, 710–11
- financial institutions 10–11, 717
- financial reporting, concepts 7, 34–5, 51, 117–46, 151–77, 240, 710–11, 720–8
- Financial Services Authority (FSA) 672–3
- financial statements 151–77, 251–3
- Finland 742, 788
- fire hazards 332–5, 428–30, 454–62, 554–8, 660
- firewalls 707–9
- fixed assets (and capital charges)
  - concepts 7, 240, 253–6, 432–6, 447, 462, 502–3, 710–11, 713
  - control objectives 253–4
  - risk/control questions 254–6
- fixed standard types of data transfers 636–44
- floats, petty cash and expenses 271–2
- flood risks 557
- floppy disk drives 497, 575
- flowcharts 48–50, 167–70
- FoI *see* freedom of information
- ‘for pay and rations’ reports, chief audit executives 83–4
- forecasts 15–16, 19–23, 219–35, 359–62
- formal procedures, informal coalitions 31–2
- France 154, 743, 788
- fraud 47, 53–4, 57–8, 84–5, 142–4, 149–50, 153–77, 242–8, 259–61, 271–2, 291, 294, 315–16, 327, 355–9, 375, 377, 392–5, 397–8, 415–24, 434–6, 446–7, 453–62, 494–501, 523, 537–41, 554–8, 566–9, 580–4, 588–604, 661–79, 683–7, 696–700, 710–11, 840–51
  - categories 150
  - collusion 149–50
  - concepts 149–50, 153–77, 259–61
  - definition 149
- ‘free-standing’ context, SAPG uses 45
- Freedom of Information Act 2000, UK 627–35, 640–1, 646, 832–3, 848–9
- Freedom of Information Acts, US 833
- freedom of information (FoI) 479–88, 497–501, 503–10, 516–23, 525–41, 581–4, 590–1, 627–35, 640–1, 646, 763–834, 848–9
  - concepts 627–35, 640–1, 763, 848–9
  - control objectives 632–3
  - definition 627, 763
  - exemptions 628, 630, 631–3
  - international legislation 627–8, 763–834, 848
  - objectives 628–9, 763
  - publication schemes 536–41, 628–35, 848–9
  - risk/control questions 633–5
  - terminology 631–2
  - time limits 630, 634
- frequency issues, internal controls 169–70
- Friedman, Milton 464
- fuel cards, petty cash and expenses 272
- functional approaches to defining the audit universe 3–26, 27, 30, 41–5, 240–75, 712–28
- gateway PCs 611–12, 707–9
- gathering *see* collection...
- GEC 97
- general ledger/management accounts
  - concepts 7, 28, 33–4, 42, 51, 240, 251–3, 462, 713
  - control objectives 251
  - risk/control questions 252–3, 462
- generally accepted accounting principles 158–60
- Georgia 743, 789
- Germany 170, 581, 744, 789–92
- Ghana 744, 792
- Gibraltar 744, 792–3
- global area networks (GANs) 609–12
- global financial crisis from 2007 82–3, 219–20
- globalisation 344
- good management practices
  - operational auditing 228–30, 251–75, 699–706
  - spreadsheets 699–706
- grant funding schemes, research and development 450–2
- Greece 744, 793–4
- grievance procedures *see* disciplinary/grievance procedures
- gross risk
  - see also* inherent...
  - concepts 101–15, 208–13
- group loyalties/rivalries, process weaknesses 30–1
- Guatemala 745, 794–5
- Guernsey 745, 795
- hacking 646, 671–9
- hardware assets 502–10, 511–13, 554–8, 566–9, 580–9, 610–12, 648–50, 694–5, 710–11
  - see also* removable media
- hazardous materials 332–8, 395–8, 428–30, 457–60, 463–75, 554–8
- health checks, IT 487, 707–9
- health insurance 7, 42, 399, 422–4, 713
  - see also* pension schemes and other benefits
  - concepts 422–4
  - control objectives 423
  - definition 422
  - risk/control questions 423–4
- health and safety at work 7, 8, 42, 318, 319, 322–4, 332–5, 339, 399, 413–15, 427–30, 454, 457–60, 554–8, 682, 713
  - see also* security; welfare...
  - concepts 413–15, 427–30, 454, 457–60, 554–8

- health and safety at work (*cont.*)  
     control objectives 427–8, 457–8  
     risk/control questions 428–30, 458–60
- health sector 10–11, 47, 717–18
- hedging 243
- Helpdesks 587, 594, 674–5, 694–5
- Herzberg's bipolar analysis of job satisfaction 190
- high level review programmes, concepts 41, 45, 147–50, 278–9, 470–5
- HMRC 622, 672–3
- holiday/sickness payments 245
- home loans 110, 194
- Hong Kong 155, 745, 795–6
- HR *see* human resource...
- Hubbard, Larry 207–10
- human resource management 3, 5, 6, 7, 27–8, 103, 113, 121–2, 399–436, 661–6, 713–14  
     *see also* personnel  
     concepts 7, 399–436, 661–6  
     control objectives 399–436, 664  
     definition 399  
     information security 661–6, 841–2  
     operational auditing 399–436  
     overview 399  
     risk/control questions 399–436, 665–6
- human resources department 7, 399, 400–4, 661–6, 713–14  
     concepts 400–4, 661–6  
     control objectives 400–1, 664  
     definition 400  
     risk/control questions 401–4, 665–6
- Human Rights Act 1998 525, 581, 592, 640–1, 646
- Hungary 746, 796
- hybrid audit universe 30
- hygiene factors of job satisfaction 190
- IBM 199
- ICAEW  
     PCAOB 157, 174–6  
     spreadsheet best practices 70
- Iceland 746, 797–8
- ICQs *see* internal control questionnaires
- ICRP, British Petroleum 199
- identity theft 672–9
- IEC *see* International Electrotechnical Commission
- IM *see* information management
- impact assessments, concepts 52–6, 101–15, 122–3, 207–8, 460–2, 471–5
- improvement programmes, operational auditing 214–35
- inaccurate information 57–74, 124–7, 242–51, 272–4, 283–9, 291–316, 493–5, 507–10, 514–23, 705–6, 710–11
- incident management 487, 520–3, 646, 671–9, 681–2, 707–9, 842  
     *see also* disaster...; information security...
- independence issues 25, 94, 151–77, 205–6, 215–35, 241–2  
     *see also* objectivity...
- India 581, 746, 798–803
- induction processes, personnel 661–2
- induction training 411–13
- informal coalitions, formal procedures 31–2
- informal organisations, concepts 189
- information asset registers  
     collection methods 505–6  
     concepts 497, 502–10, 515–23, 527–41, 681–7, 700–1, 715, 725, 847, 850  
     control objectives 505–6, 507–8  
     costs and benefits analysis 507–10  
     data fields 504–6, 700  
     definition 502–7  
     ownership issues 504–5, 507–10, 701–2, 847  
     responsibilities 503, 507–10, 847, 851  
     risk/control questions 509–10  
     security issues 504–10, 847
- information business process, concepts 34
- Information Commissioner 617–26, 628–35, 759–60  
     *see also* data protection; freedom of information
- 'information and communication' component, COSO  
     internal control framework 120–1, 124–7, 157–8, 170–7
- information definitions 543–5, 836
- information management (IM) 479–88, 496–501, 506–10, 514–23, 524–5, 587–9, 613–15, 645–7, 715, 725, 836, 839  
     *see also* knowledge...; records...  
     control objectives 521–2  
     definition 514–16, 836  
     risk/control questions 521–3
- information requirements 12–14, 47–50, 82–4, 120–1, 124–7, 151–77, 188–9, 208–13, 242–3, 272–4, 286–9, 401–36, 448–52, 502–10, 514–23, 613–15, 710–11  
     *see also* financial information...  
     material information 151–77  
     subsidiaries 277–84, 366–8
- information security incidents 487, 520–3, 646, 671–9, 681–3, 707–9, 841–2  
     concepts 520–3, 671–9, 681–3, 841–2  
     control objectives 676–7  
     examples 671–3, 674–5, 681–3  
     management 487, 520–3, 673–9, 681–2  
     risk/control questions 677–9  
     statistics 671–2  
     UK examples 672–3  
     US examples 673, 682–3
- information sharing agreements (ISAs) 639–44
- information technology (IT) 6, 8–9, 43–4, 56–74, 103, 113, 121–4, 136–7, 179–81, 188–9, 192, 195, 233–4, 479–711, 712–28  
     *see also* facilities management; hardware...; software...  
     accounting 710–11  
     back-up systems 8, 43–4, 67–74, 486, 497–501, 505–10, 521–3, 537–41, 558, 562–5, 584, 588–9, 846
- BACS 245, 261, 487, 696–8

- best practices 480–8, 521–3
- capacity management 486, 497, 511–13, 520–3, 715, 725, 846
- concepts 479–88, 712–28
- contingency plans 497–501, 512–13, 528–41, 561, 658–60, 671–9, 689–90, 707–9
- data retention and disposal 487, 497, 524–41, 562–5, 620–6, 638–44, 680–7, 851
- databases 9, 43, 57–74, 136–7, 502–10, 544–53, 613–15
- EDI 43–4, 198, 248–50, 487, 688–90
- emails 487, 497, 520–3, 581–4, 590–7, 691–3, 841
- health checks 487, 707–9
- Helpdesks 587, 594, 674–5, 694–5
- human resource information security 661–6, 667–70, 841–2
- information security incidents 487, 520–3, 646, 671–9, 681–3, 707–9, 841–2
- Internet 10, 35–6, 40, 44, 92–3, 121–2, 479, 487, 497, 581, 593–4, 598–604, 609–10, 646, 667–70, 842–3
- legislation 9, 43–4, 404–7, 479–88, 496–501, 514–23, 525–41, 581–4, 645–7, 707–9, 729–834
- logging systems 487, 576–9, 588–9, 667–70, 694–5
- organisational structures 8, 486, 493–5, 524–41, 715, 725
- overview 486–8
- ownership issues 504–5, 507–10, 524–41, 578–9, 701–2, 838
- personal computers 8–9, 43–4, 486–8, 562–5, 570–5, 580–9
- policies 479–88, 489–501, 506–10, 511–13, 514–41, 554–8, 566–9, 576–9, 580–4, 585–9, 591–7, 599–604, 715, 725, 839–51
- processing operations 559–61
- remote working 487, 497–501, 520–3, 585–9, 844
- removable media 487, 497–501, 520–3, 533, 566–9, 844–5
- responsibilities 493–5, 497–501, 503, 518–23, 524–41, 556–8, 563–5, 585–9, 601–4, 616–26, 627–44, 645–7, 661–6, 691–3, 851
- SAPG 715–16, 725–7
- service management 483–4
- sites and infrastructure 486, 554–8, 715, 725, 843
- spreadsheets 40, 53–4, 56–74, 487, 699–706
- standards 480–8, 493–5, 515–41, 581–4, 645–7, 652–4, 701–6
- strategic planning 8, 486, 489–92, 511–13, 582–4, 715, 725
- system development 487, 651–7, 699–706
- systems and operating software 9, 43–4, 64, 71–4, 487, 559–61, 570–5, 667–70
- terms of reference 493–5
- user support services 487, 694–5
- inherent risk
  - see also* control matrices; gross...; risk
  - concepts 52–4, 55–6, 57–74, 101–15, 122–3, 208–13, 275
  - definition 52–3, 101
- inputs
  - operational auditing evaluations 219–35
  - systems concepts 131–5
  - three Es (effectiveness, efficiency, and economy) 15–16, 19–23, 29–30, 219–35
  - VAT 261–3
- Institute of Internal Auditors (IIA) 3–5, 11–12, 16–19, 21–6, 76–82, 93, 95–8, 115, 121–2, 139–41, 157, 171, 176–7, 204, 210, 212, 214–19, 225, 229, 232–5, 570
- 1000 (Purpose, Authority, and Responsibility) 217
- 1010 (Recognition of the Definition of Internal Auditing...) 217
- 1100 (Independence and Objectivity) 25, 94, 176, 215
- 1130 17, 171
- 1210 16
- 2010 176, 212, 234
- 2020 17
- 2100 (Nature of Work) 76–7, 93
- 2110 (Governance) 16, 25–6, 77–82
- 2120 (Risk Management) 77–9, 95–9, 176
- 2130 (Control) 77–9
- 2210 176
- 2600 25
- CCSA programme 204, 210
- internal control framework 139–41, 157, 176
- Quality Assurance and Improvement Program 214–17
- standards 3, 11–12, 16–19, 21–6, 76–80, 95–8, 115, 121–2, 139–41, 171, 176, 214–17, 225, 229, 232–5
- insurance cover 296, 385–98, 413–15, 430, 434–6, 457, 458–62, 555–8, 671–9, 713, 721
- see also* security
- claims 460–2
- concepts 296, 389–92, 454, 460–2, 555–8
- contracting 296, 389–92
- control objectives 460–1
- costs and benefits analysis 460–2
- distribution 385–98
- risk/control questions 461–2
- types 460–2
- integrity business process, concepts 34, 96–115, 121–4, 147–50, 248, 493–5, 610–12
- intellectual property 345–8, 366, 439–42, 450–2, 453–62, 533, 594–7, 646, 672–9
- see also* patents
- inter-group rivalries, intra-group loyalties 30–2
- interim payments for contracts, concepts 9, 44, 290, 308–13
- internal auditors, CIA designation 204
- internal audits *see* operational auditing
- internal checks, concepts 116–17
- internal control questionnaires (ICQs) 40–74
- internal controls
  - see also* Sarbanes-Oxley Act 2002
  - BPR 181

- internal controls (*cont.*)
- business processes 34–9, 116–46
  - categories of control 137–9, 144, 168–70
  - CoCo framework 117–18, 129–30, 141–3, 144, 157–8, 208–9
  - concepts 3–26, 29–30, 34–9, 40–74, 75–94, 96–8, 116–46, 147–50, 151–77, 201–13, 226–35, 281–4, 470–5, 718
  - contemporary understanding 116, 117–18
  - control-effectiveness measurements 127–8, 141–3, 151–77, 209–13
  - corporate governance 76–94
  - COSO framework 117–28, 140, 142, 144, 157–77
  - definitions 5–6, 15, 77–9, 116–20, 128–30, 140–1
  - division-with-supervision opportunities 135–7, 142–3, 150
  - failures 141–3, 151–77
  - frequency issues 169–70
  - IIA framework 139–41, 157, 176
  - joint ventures 281–4
  - objectives 77–81, 96–9, 116–20, 123–30, 139–41, 151–77
  - process issues 143–4
  - risk management 75–94, 96–8, 112–15, 122–3, 137–42, 147–50, 151–77, 232–5
  - ‘Rubik cube’ 120–1
  - SAPG 718
  - ship analogy 119–20
  - systems/cybernetics model 130–5
  - Turnbull framework 117–18, 120, 128–9, 140–2, 144, 157–8, 170–1
- internal environment 98–115
- internal governance processes, concepts 75, 78, 81–2, 84–7
- internal telephone directories 28
- International Electrotechnical Commission (IEC)
- see also* ISO...
  - background information 480–8
- international legislation 616, 627–8, 729–834, 848
- data protection 616, 729–62, 848
  - freedom of information (FoI) 627–8, 763–834, 848
- International Professional Practices Framework (IPPF) 76, 215, 225
- Internet 10, 35–6, 40, 44, 92–3, 121–2, 479, 487, 497, 581, 593–4, 598–604, 609–10, 646, 667–70, 842–3
- see also* information technology
  - access controls 599–604, 667–70, 842–3
  - concepts 598–604, 609–10, 646, 667, 842–3
  - control objectives 602
  - historical background 598–9
  - policies 599–604, 842–3
  - risk/control questions 603–4
  - statistics 598–9
  - websites 10, 35–6, 40, 44, 92–3, 218, 712, 729–834
- interviews 57–8
- intra-group loyalties, inter-group rivalries 30–2
- intranets 546–8
- inventories 7–8, 33–4, 42, 51, 195–8, 240, 266–8, 321, 327, 362–6, 380–2, 383–98, 681, 713
- see also* stock...
  - concepts 7–8, 195–8, 266–8, 383–98
  - control objectives 266
  - key spreadsheets 700–1
  - risk/control questions 266–8
  - valuations 266–8
- investigative category of control 139, 144
- investments
- concepts 7, 240, 274–5, 713
  - control objectives 274
  - risk/control questions 274–5
- investors 33–4, 42, 93
- invoices 246–51, 268, 354–5, 372–5, 389–92, 446–7, 688–90
- see also* accounts payable; accounts receivable
- inward focus of benchmarking 24
- IP addressable devices 707
- Iran 747, 803
- Iraq 747, 803
- Ireland (Eire) 747, 804
- irregular tests of information flows, operational auditing
- definition 14
- ISAs *see* information sharing agreements
- Isle of Man 747, 804
- ISO 182, 183–4, 466–7, 480–8, 496, 526, 640, 707
- see also* British Standards Institute
  - 14000 series 466–7, 475
  - 5489 (Information and Documentation–Records Management) 484–6, 526
  - background information 182, 183–4, 466–7, 480–8
- ISO/IEC 17799 481, 526, 640
- ISO/IEC 20000–1 484
- ISO/IEC 27000 series 480–4, 526, 640, 707
- ISO/IEC, background 480–8, 496
- Israel 747–8, 804
- IT *see* information technology
- Italy 748, 804–5
- Jaenicke, H.R. 34
- Jamaica 748, 805–6
- Japan 154, 195, 466, 581, 748, 806
- JCL 560–1, 575
- Jersey 748, 807
- Jikoda (‘stop everything...’) 195–6
- JIT... *see* just-in-time...
- job descriptions/specifications 144, 149, 401–4, 405–7, 493–5
- job satisfaction 190–1
- Johnson, K.P. 34
- Joint Information Systems Committee (JISC) 534
- joint ventures
- concepts 279–84
  - cultural issues 280–1
  - definition 279–80
- just-in-time management (JIT)
- concepts 178, 195–8, 285, 317, 383
  - costs and benefits analysis 197–8
  - cultural issues 196
  - definition 195

- operational auditing 196–8, 285
- just-in-time purchasing (JITP), concepts 196–8, 285
- Kanban* cards 196–8
- Kazakhstan 807
- Kenya 749, 808
- key issues, SAPG questions 46–50
- keying errors 57–74, 699–700
- King Report on Corporate Governance, South Africa 140, 141
- KM *see* knowledge management
- know-how 543–53, 838
- knowledge management (KM)
  - see also* data...; information...
  - benefits 542–5
  - best practices 485–8
  - BSI guidance publications 486
  - concepts 479–88, 497–501, 519–23, 542–53, 715, 725, 836–8, 849–50
  - control objectives 550–1
  - definitions 485–6, 542–5, 836–8, 849
  - information sources 542–6
  - lessons learned 549–53
  - life-cycle issues 544–5, 547–9
  - policies 549–53, 849–50
  - responsibilities 550–3, 849–50, 851
  - risk/control questions 551–3
  - tacit/explicit knowledge 544–53, 836, 838
  - why-what-who-how questions 549–50
- knowledge/skills/competencies requirements of auditors 16–18, 86–7, 158–60, 218, 233–4
- labour relations 7, 399, 400–4, 430–2, 714
  - concepts 430–2
  - control objectives 431
  - risk/control questions 431–2
- LANs *see* local area networks
- laptop computers 580–9, 672–3
- Latvia 749, 809
- law and regulatory compliance
  - see also* compliance...; legislation; regulations
  - concepts 4–5, 8, 318, 338–9, 665–6, 714
  - control objectives 338
  - risk/control questions 338–9
- law of requisite variety 131–5
- leadership qualities 118–20
- learning 129–30, 144, 208–13, 542–53
- least cost basis 22–3
- Lebanon 749, 809–10
- legal departments 6, 27, 41, 43, 368, 450–2, 645–7, 712–15, 721
- legislation 46, 77–9, 96–115, 117–46, 242–3, 261–6, 272–5, 287–9, 291–316, 319–42, 363–82, 385–98, 400–36, 439–52, 463–75, 479–88, 496–501, 514–23, 524–41, 602–4, 616–35, 640–4, 645–7, 674–9, 680–7, 707–11, 712–15, 721, 729–834
  - see also* individual Acts
  - data protection 9, 43–4, 404–7, 479–88, 496–501, 514–23, 524–41, 581–4, 590–7, 616–26, 631–2, 639–44, 646, 729–62, 835, 838, 842, 848
  - freedom of information 627–8, 763–834, 848
  - international legislation 616, 627–8, 729–834, 848
  - IT 9, 43–4, 404–7, 479–88, 496–501, 514–23, 525–41, 581–4, 645–7, 707–9, 729–834
  - list of IT legislation 525–6, 581, 645–7, 729–834
  - records management 524–41, 646–7, 680–7, 849
- Lesotho 749, 810
- lessons learned 549–53
- Liberia 749, 810–11
- Libya 749, 811–12
- Liechtenstein 749, 812
- life-cycle issues 372–5, 468–75, 544–5, 547–9, 661–6, 680–7
- Likert's linking pins, concepts 31–2
- Limitation Act 1980 646
- line marketing, definition 344
- linking pins, concepts 31–2
- listed companies 151–77
- Listing Rules 176
- Lithuania 749, 812
- loans 10–11, 110, 194, 259–61
- local area networks (LANs) 9, 43–4, 489, 584, 609–12, 673, 693
- Local Government Acts 646
- logging systems 487, 576–9, 588–9, 667–70, 694–5
- logical security *see* system access controls
- logistics 8, 42, 383, 384–8, 714
  - see also* distribution
- London listings 155
- Luxembourg 749, 812–13
- Macedonia 750, 813
- McRae, Elizabeth 218
- maintenance 8, 9, 44, 318, 339–42, 377–80, 435–6, 487, 504–10, 528–41, 570–5, 605–8, 651–7, 699–706, 714
  - see also* facilities, plant and equipment; software...
  - contracting obligations 9, 44
  - control objectives 340, 377–8
  - MISs 57–74
  - production/manufacturing 8, 318, 339–42
  - records management 528–41, 849
  - risk/control questions 340–2, 378–80
- maintenance and servicing 8, 343, 377–80, 715
  - see also* after sales support
  - concepts 377–80
  - control objectives 377–8
  - risk/control questions 378–80
- Malaysia 750, 814
- malicious software 9, 43, 497–501, 520–3, 563–9, 570–5, 583–4, 590–7, 601–4, 671–9, 691–3, 707–9, 841, 846
  - see also* malware; spyware; viruses
- malpractice 57–74, 84–5, 142–4, 149–50, 151–77, 242–8, 259–61, 271–2, 288–9, 291, 294, 298–9, 315–16, 327, 352–9, 363–6, 375, 377, 389–95, 397–8, 415–24, 434–6, 446–7, 453–62, 494–501, 523, 537–41, 554–8, 566–9, 580–4, 588–604, 661–79, 683–7, 696–700, 710–11, 840–51

- Malta 750, 814
- malware 9, 43, 497–501, 520–3, 563–9, 570–5, 596–7, 601–4, 671–9, 691–3, 707–9
- management  
*see also* Sarbanes-Oxley Act 2002  
 back-up and media management 8, 43–4, 67–74, 486, 497–501, 505–10, 521–3, 537–41, 558, 562–5, 584, 588–9, 846  
 business management techniques 178–98  
 capacity management 486, 497, 511–13, 520–3, 846  
 concealed risks 107–10  
 CSAs 199–213  
 data protection 9, 43–4, 404–7, 479–88, 496–501, 503–10, 514–23, 525–41, 562–5, 581–4, 590–7, 616–26, 631–2, 639–44, 848  
 delayering considerations 178, 187–9  
 EDI 43–4, 198, 248–50, 487, 688–90  
 emails 487, 497, 520–3, 581–4, 590–7, 691–3  
 environmental issues 463–75  
 ethics/competencies 147–50, 158–77, 209–13, 215–35  
 facilities management 9, 43–4, 192, 648–50  
 fraud 149–50, 153–77  
 freedom of information 479–88, 497–501, 503–10, 516–23, 525–41, 581–4, 590–1, 627–35, 640–1, 646–7, 763–834, 848  
 human resource information security 661–6, 667–70, 841–2  
 human resource management 3, 5, 6, 7, 27–8, 103, 113, 121–2, 399–436  
 information asset registers 502–10, 515–23, 527–41, 681–7, 700–1, 847, 850  
 information management 479–88, 496–501, 505–10, 514–23  
 information security incidents 487, 520–3, 671–9, 681–2, 707–9, 841–2  
 internal controls 3–26, 29–30, 34–9, 40–74, 75–94, 96–8, 116–46, 147–50, 151–77, 201–13  
 Internet 10, 35–6, 40, 44, 92–3, 121–2, 479, 487, 581, 593–4, 598–604, 842–3  
 IT overview 479–88  
 joint ventures 279–84  
 knowledge management 479–88, 497–501, 519–23, 542–53, 849–50  
 legal responsibilities 645–7, 844  
 objectives 12–14, 16–17, 29–30, 47, 118, 147–50, 201–13, 214–35  
 records management 479–88, 496–501, 502–10, 511–13, 515, 517–23, 524–41, 680–7, 849  
 software maintenance/development controls 9, 43–4, 64, 67–74, 487, 605–8, 651–7, 699–706  
 software selection 655–7, 845  
 span of control 118–20, 187–8  
 spreadsheets 40, 53–4, 56–74, 487, 699–706  
 subsidiaries 3, 265, 276–84, 366–8  
 system access controls 8, 487, 576–9, 661–6, 707–9  
 system development 487, 651–7, 699–706  
 systems and operating software 570–5, 667–70  
 user support services 487, 694–5
- management and administration 6–7, 41, 51, 712–13, 721
- management controls *see* internal controls
- management information systems (MISs)  
 concepts 41–4, 51, 56–74, 125–7, 362, 367, 368, 548–9, 710–11, 721  
 control matrices 56–74  
 risk exposures 56–74
- managing customers as strategic assets (MCSA) 344
- mandatory/regulatory/statutory data transfers 636–44
- manpower and succession planning  
 concepts 7, 399, 407, 408–10, 713  
 control objectives 408  
 risk/control questions 408–10
- manual logs, concepts 667–70
- manufacturing *see* production...
- Marconi 97–8
- market research  
 concepts 8, 43, 346–7, 348–50, 442, 714  
 control objectives 343–9  
 costs and benefits analysis 349–50  
 definition 348  
 risk/control questions 349–50
- market shares 268–70, 279, 363–4, 389–92
- marketing and sales 3, 5–6, 8, 27–8, 32–5, 43, 51, 113, 136, 194, 343–82, 438–42, 620, 714, 724  
*see also* after sales...; agents; distributors; order processing; pricing...; product...; promotion...; sales...
- concepts 8, 343–82, 620, 714, 724  
 control objectives 344–81  
 data protection 620–6  
 definition 343–4  
 overview 343–4  
 parent company relationships 366–8  
 risk/control questions 344–81  
 SAPG 714, 724
- Maslow's hierarchy of needs 190–1
- material information 151–77
- 'material weaknesses', definitions 153, 156–7, 172
- materials and energy  
 concepts 8, 318, 327–30, 392–5, 463–75, 714  
 hazardous materials 332–8, 395–8, 428–30, 457–60, 463–75, 554–8
- maturity models, operational auditing 218–19
- Maxwell, Robert 415
- media 8, 43–4, 67–74, 91, 486, 496–501, 505–10, 520–3, 537–41, 558, 562–5, 713, 721
- metadata 497, 502–10, 515–23, 527–41, 837  
*see also* information asset registers
- metropolitan area networks (MANs) 609–12
- Mexico 751, 815
- milestones 294–5, 306–16, 510
- minutes of meetings 128
- mission 71–4, 95–8, 112–15, 209–13
- misstatements 109, 151–77, 259–61, 271–2, 315–16
- mobile phones 585–9
- Mongolia 751, 816



- monitoring 7, 8, 14, 51, 71–4, 99–115, 120–1, 127–30, 142, 144, 157–8, 170–7, 185–7, 208–13, 214–15, 223–35, 240, 256–8, 306–8, 343, 346, 359–62, 437, 442–5, 487, 517–23, 592–7, 652–4, 667–70, 694–5, 710–11  
   emails 592–7  
   information flows 14, 99–115, 120–1, 127–30, 170–1, 208–13, 272–4, 667–70  
   information management 517–23, 667–70  
   logging systems 487, 576–9, 588–9, 667–70, 694–5  
   ongoing monitoring 214–35  
   project appraisal and monitoring 8, 437, 442–5, 651–4  
   risk matrices 102–6  
   sales performance and monitoring 8, 343, 346, 359–62  
   ‘monitoring’ component, COSO internal control framework 120–1, 127–8, 142, 144, 157–8, 170–7  
 moral hazard 144  
 mortgages 10, 110  
 motivation levels 71–4, 120–2, 148–50, 181, 184–7, 190–1, 196–8, 203–4, 400–36, 547  
 Mozambique 752, 817  
 multinational enterprises 5–6, 12–14  
  
 NAID 684–5  
 Namibia 752, 817  
 National Environmental Policy Act 465–6  
 Nationwide Building Society 672  
 Nepal 752, 817–18  
 NESTOR 534  
 Netherlands 534, 752, 818–19  
 nett risk *see* residual risk  
 networks 9, 43–4, 487, 489, 511–13, 546–53, 554–8, 580–9, 609–12, 673, 693, 707–9  
   concepts 609–12, 707–9  
   control objectives 610–11  
   MISs 68–74  
   risk/control questions 611–12  
   statistics 609–10  
   types 609–10  
 new products 8, 34–5, 343, 345–8, 438–52, 473  
   *see also* product development  
 New Zealand 752  
 news groups 600–4  
 Nicaragua 752, 820  
 Nigeria 752, 820  
 non-audit services 163–77  
 nonexecutive directors 87–90, 127–8  
 Norway 752, 820–1  
 Novell networks 68  
 nuclear industry 109  
 ‘number of auditors per 1000 staff’, operational auditing evaluations 223–33  
  
 objectives  
   mission 112–15  
   perspectives 12–14, 16–17, 25, 64, 71–4  
   ‘triple bottom line’ objectives 464, 473  
  
 objectivity issues 14, 17, 25, 94, 176, 205–6, 215–35  
   *see also* independence...  
 Obscene Publications Acts 646  
 obsolescence 380–2, 532–41, 681–7  
 omissions 57–74, 151–77  
 ongoing monitoring, operational auditing 214–35  
 Open Document Management API (ODMA) 531–2  
 open systems, concepts 131–5  
 operational auditing  
   added value 21–3, 76, 211–12, 219–35, 364–6, 370–1, 391–2  
   approaches 3–26  
   assessments 214–35, 470  
   audit approaches 12–16  
   ‘budget/actual comparisons’ 223–33  
   business management techniques 178–98  
   business processes 3–4, 27–39, 240, 712–28  
   Charters 217–35  
   concepts 3–26, 27–39, 76–94, 99–115, 170–3, 178–98, 201–13, 214–35, 470, 712–28  
   corporate governance 3, 5–6, 9–10, 17, 22, 25–6, 29–30, 34, 44, 75–94, 176–7, 205, 232–5, 470–5, 509–10, 718  
   costs and benefits analysis 219–35  
   CSAs 18–19, 30, 41, 102–3, 128, 199–213, 718  
   data protection 9, 43–4, 404–7, 479–88, 496–501, 503–10, 514–23, 525–41, 562–5, 581–4, 590–7, 616–26, 631–2, 639–44, 729–62, 848  
   data retention and disposal 487, 497, 524–41, 562–5, 620–6, 638–44, 680–7, 851  
   data transfers and sharing 515–23, 542–53, 636–44, 688–90, 704–6, 850  
   databases 9, 43, 57–74, 136–7, 502–10, 544–53, 613–15  
   definitions 3–5, 12–13, 14, 21–2, 76, 95, 835–8  
   EDI 43–4, 198, 248–50, 487, 688–90  
   emails 487, 497, 520–3, 581–4, 590–7, 691–3  
   empowerment considerations 191  
   environmental issues 463–75  
   evaluations 214–35  
   external reviews 214, 216–17  
   facilitation roles 201–6, 212  
   finance and accounting 3, 6, 7, 27, 32–5, 42, 117, 143–5, 192, 197–8, 239–75, 713, 722  
   freedom of information 479–88, 497–501, 503–10, 516–23, 525–41, 581–4, 590–1, 627–35, 763–834, 848  
   functional approaches 3–26, 27, 30, 41–5, 240–75, 712–28  
   good management practices 228–30, 251–75, 699–706  
   human resource information security 661–6, 667–70, 841–2  
   improvement programmes 214–35  
   information asset registers 497, 502–10, 700–1, 847, 850  
   information management 479–88, 496–501, 506–10, 514–23

operational auditing (*cont.*)

- information requirements 12–14, 47–50, 82–4, 120–1, 124–7, 170–1, 272–4, 514–23, 710–11
  - information security incidents 487, 520–3, 671–9, 707–9, 841–2
  - input performance measures 221–35
  - Internet 10, 35–6, 40, 44, 92–3, 121–2, 479, 487, 581, 593–4, 598–604, 842–3
  - IT overview 479–88, 715–16
  - IT strategic planning 489–92, 511–13, 582–4, 715, 725
  - joint ventures 282–4
  - knowledge management 479–88, 497–501, 519–23, 542–53, 849–50
  - legal responsibilities 645–7, 844
  - management and administration 6–7, 41, 51, 712–13, 721
  - maturity models 218–19
  - networks 487, 511–13, 546–53, 554–8, 580–9, 609–12, 707–9
  - ‘number of auditors per 1000 staff’ 223–8
  - objectives 12–14, 16–17, 25, 230–5, 470
  - ongoing monitoring 214–35
  - output performance evaluations 219–35
  - performance/productivity measurement systems 9, 19–23, 31, 78, 84, 85, 219–35, 290, 306–8, 313–16, 319–42, 359–66, 424–7
  - periodic internal reviews 214–35
  - profitability contributions 219–35
  - quality assurance 182–7, 214–35, 330–2
  - quantitative/quasi-quantitative/qualitative performance measures 221–8
  - ‘ratio of payroll to other costs’ 223–33
  - ‘ratio of productive/unproductive audit time’ 223–33
  - recessions 82–3, 219–20
  - recommendations 226–35
  - records management 479–88, 495–501, 502–10, 511–13, 515, 517–23, 524–41, 680–7, 849
  - responsibilities 29–30, 47, 87, 100, 112–15, 118–20, 125–30, 135–7, 144, 148–50, 170–3, 201–2, 493–5, 497–501, 503, 518–23, 661–6, 691–3, 851
  - reviews 214–35
  - SAPG 10, 35–6, 40–74, 240–1, 285, 318, 345, 384, 400, 438, 454, 470, 488, 712–28
  - scope 3–12, 16–17, 27–39, 152, 164, 166–7, 170–3, 201–2, 218–35, 239–40, 469–75, 707–9
  - software maintenance/development controls 9, 43–4, 64, 67–74, 487, 605–8, 651–7, 699–706
  - software selection 655–7, 845
  - spreadsheets 40, 53–4, 56–74, 487, 699–706
  - subsidiaries 3, 265, 276–84, 366–8
  - system access controls 8, 487, 576–9, 661–6, 707–9
  - system development 487, 651–7, 699–706
  - systems and operating software 570–5, 667–70
  - value for money auditing 21–3, 230–3, 353
  - weaknesses 217–18
- operational level of risk, concepts 52

## operational review programmes, development issues 40–74

## operations logs for MISs 68–74

## operations and resource management

*see also* production/manufacturing

concepts 317–42

## opportunities, risk management 111, 113–15, 226–8

## optical disks 566–7

## order processing 8, 343, 362, 366, 371–5, 385–8, 398, 714

*see also* accounts receivable; credit-granting...;

debtors; marketing...

concepts 362, 366, 371–5, 388

control objectives 372

definition 371–2

life-cycle issues 372–5

risk/control questions 373–5

## organisational structures

concepts 5–6, 8, 31–2, 47–50, 110, 118–22, 178–98, 486, 493–5, 524–41

IT organisation 8, 486, 493–5, 524–41

## organising 5–6, 116, 118–20

## out-of-date information 57–74

## out-of-stock situations 380–2, 392–5

## outputs

operational auditing evaluations 219–35

systems concepts 131–5

three Es (effectiveness, efficiency, and economy)

15–16, 19–23, 29–30, 219–35

VAT 261–3

## outsourcing considerations 18–19, 22–3, 116, 144, 178, 191–5, 220–1, 234, 648–50, 651–7, 683–7, 716–17, 726–8

*see also* contracting...; facilities management

cleaning firms 192, 193

core/non-core activities 193–4, 195

costs and benefits analysis 192–4, 220–1, 648–50, 655–7

cultural issues 192, 193, 220–1

definition 191–2

disposal of records 683–7

personnel impacts 192, 193–4

public sector 192

risk/control questions 192, 193, 194–5, 220–1, 649–50

## outward focus of benchmarking 24

## overdrafts 258–61

## overhead costs 317–42

## overseas operating units 3

## ownership issues

information asset registers 504–5, 507–10, 701–2, 847

IT 504–5, 507–10, 524–41, 578–9, 701–2, 838

policies 498–501, 578–9, 701–2

## P11D returns 424

## packaging, environmental issues 468–75

## Pakistan 753, 821

## paper records, retention issues 680–7

- parameters to MISs 57–74
- parent companies  
     *see also* subsidiaries  
         concepts 265, 276–84, 366–8, 714
- passwords 58–74, 518–23, 527–41, 576–9, 585–9, 601–4, 623–6, 638–44, 707–9, 843
- patch management 487, 520–3, 570–5, 707–9, 845–6
- patents 345–8, 439–42, 450–2, 581, 594–5, 646  
     *see also* intellectual property
- payments business process, concepts 34–5
- payroll  
     *see also* remuneration  
         concepts 7, 27–8, 33–4, 42, 53–4, 223–33, 240, 243–5, 362, 405–7, 415, 713  
         control objectives 243–4  
         risk/control questions 244–5, 362
- PCAOB *see* Public Company Accounting Oversight Board
- PCs *see* personal computers
- PDAs 567, 580–9
- peer groups, knowledge management 546–53
- pension schemes and other benefits 7, 42, 399, 415–24  
     *see also* health insurance  
         concepts 415–22  
         control objectives 416–17  
         ethics 415–22  
         risk/control questions 417–22
- performance category of control 138
- performance-related compensation schemes  
     *see also* pension schemes...  
         concepts 415–22, 713
- performance/productivity measurement systems 9, 19–23, 31, 78, 84, 85, 219–35, 290, 306–8, 313–16, 319–42, 359–66, 424–7  
     concepts 8, 9, 19–23, 31, 44, 74, 78, 84, 85, 209–13, 219–35, 270, 290, 306–8, 313–16, 319–42, 343, 346, 359–66, 424–7, 652–7
- contracting 9, 290, 306–8, 315–16, 385–92
- distributors 362–6, 388–92
- milestones 294–5, 306–16
- personnel 234, 314–16, 324–7
- policies 20–1, 85
- reviews of project outturn/performance 313–16
- sales performance and monitoring 8, 343, 346, 359–62
- staff appraisals 7, 234, 314–16, 324–7, 399, 400–4, 413, 424–7
- three Es of effectiveness, efficiency, and economy 19–23, 77–9, 84, 85, 117–46, 215–35
- perimeters and external environs, IT sites and infrastructure 555–8, 843
- periodic internal reviews, operational auditing 214–35
- personal computers (PCs) 8–9, 43–4, 486–8, 562–5, 570–5, 580–9, 608, 623–6, 699–706, 840–1  
     *see also* information technology  
         concepts 580–4  
         control objectives 582  
         risk/control questions 582–4  
         statistics 580–1
- personal data, data protection 617–26, 636–44, 646, 729–62, 837, 848
- personnel 3–8, 15–16, 20–1, 27–8, 33–4, 42, 53–4, 71–4, 84–5, 91–4, 112–15, 118–22, 125, 144, 147–50, 178, 188, 189–98, 241–5, 291, 294, 317–42, 343, 355–9, 399–436, 454–62, 489–501, 510, 516–41, 661–6, 713–14, 722–3  
     *see also* health...; human resource...; manpower...; pension schemes...; recruitment...; training...  
         absenteeism rates 325–7, 401–4, 425–7
- Codes of Conduct 148–9
- company vehicles 7, 399, 432–6, 556–8
- concepts 7, 399–436, 661–6, 713–14, 722–3
- contracts of employment 405–7, 441–2
- control objectives 325, 399–436, 664
- data protection 616–26, 631–2, 639–44
- definition 399–400
- disciplinary/grievance procedures 7, 85, 149, 399, 400–4, 424–7, 594–7, 604, 641–4
- efficiency issues 15–16, 20–1
- emails 487, 497, 520–3, 581–4, 590–7
- empowerment considerations 178, 188, 189–91, 195–6
- fraud 149–50, 242–5, 291, 294, 327, 355–9, 494–5, 588–97
- freedom of information 631–5, 848
- group loyalties/rivalries 30–1
- induction processes 661–2
- information security 487, 520–3, 646, 661–6, 667–70, 671–9, 841–2
- Internet 10, 35–6, 40, 44, 92–3, 121–2, 479, 487, 581, 593–4, 598–604, 842–3
- JIT 195–8
- job descriptions/specifications 144, 149, 401–4, 405–7, 493–5
- job satisfaction 190–1
- labour relations 7, 399, 400–4, 430–2
- legal responsibilities 645–7, 844
- maintenance 8, 9, 44, 318, 339–42
- motivation levels 71–4, 120–2, 148–50, 181, 184–7, 190–1, 196–8, 203–4, 400–36, 547
- outsourcing impacts 192, 193–4
- overview 399
- payroll 7, 27–8, 33–4, 42, 53–4, 223–33, 240, 243–5
- performance/productivity measurement systems 234, 314–16, 324–7
- production/manufacturing 317–42
- quality assurance systems 182–7
- remote working 487, 497–501, 520–3, 585–9, 844
- removable media 487, 497–501, 520–3, 533, 566–9, 672–3, 844–5
- remuneration 325–7, 355–62, 400–7, 415–22
- retention rates 149–50, 325–7, 401–4, 441
- risk/control questions 325–7, 399–436, 665–6
- sales management 8, 343, 355–9
- SAPG 713–14, 722–3
- security policies 495, 496–501, 520–3, 554–8, 661–6, 839–43, 849
- share schemes 415–22

personnel (*cont.*)

- spreadsheets 40, 53–4, 56–74, 487, 699–706
  - staff appraisals 7, 234, 314–16, 324–7, 399, 400–4, 413, 424–7
  - succession planning 7, 399, 407, 408–10
  - system access controls 8, 487, 576–9, 661–6, 667–70, 707–9
  - tacit knowledge 544–53
  - termination of employment 400–4, 410, 425–7, 662–6, 841–2
  - turnover rates 149–50, 325–7, 401–4
  - user support services 487, 694–5
  - welfare 7, 399, 400–4, 413–15
  - whistleblowing policies 84–5, 121–2, 149
- Peru 753, 821
- petty cash and expenses, concepts 7, 240, 270–2, 713
- Philippines 753, 822
- physical security 332–5, 428–30, 454–62, 486, 495, 496–501, 520–3, 554–8, 588–9, 638–44, 658–66, 667–70, 681–7, 707–9, 837, 849
- see also* security
- control objectives 556, 664
  - fire hazards 332–5, 428–30, 454–62, 554–8, 660
  - IT health checks 487, 707–9
  - IT sites and infrastructure 486, 487, 520–3, 554–8, 658–60, 671–9, 681–7, 715, 725, 843
  - risk/control questions 557–8, 665–6
  - security policies 495, 496–501, 520–3, 554–8, 661–6, 839–43, 849
- pilot exercises 71–4
- PLANETS Project 535
- planning 5–6, 8, 11–16, 19–21, 34–5, 41–5, 110, 116, 118–20, 207, 219–35, 318–21, 350, 359–61, 442, 712–14, 721
- control matrices 64, 71–4
  - control process concepts 8, 34–5, 219–35, 318–21, 350
  - production control concepts 8, 318–21, 714
  - three Es (effectiveness, efficiency, and economy) 15–16, 19–23, 219–35
- plant and equipment
- see also* facilities, plant and equipment
- concepts 8, 318, 319–24, 339–42, 427–30, 445–7, 457–60, 714, 715
  - R&D equipment 8, 437, 445–7
- Poland 753, 822
- policies 20–1, 81–4, 85, 87–90, 211, 241–2, 332–5, 428–30, 457–60, 479–88, 489–501, 506–10, 511–13, 514–41, 549–58, 566–9, 839–51
- see also* procedures
- boards of directors 81–4, 87–90, 211
  - Data Protection Act 1998 616–26, 639–44, 646, 759–60, 835, 838, 842, 848
  - emails 591–7, 841
  - freedom of information 628–35, 763–834, 848
  - information management 479–88, 496–501, 506–10, 514–23
  - Internet 599–604, 842–3

- IT 479–88, 489–501, 506–10, 511–13, 514–41, 554–8, 566–9, 576–9, 580–4, 585–9, 591–7, 599–604, 839–51
  - knowledge management 549–53, 849–50
  - ownership issues 498–501, 578–9, 701–2
  - performance/productivity measurement systems 20–1, 85
  - personal computers 580–4
  - remote working 585–9, 844
  - removable media 566–9, 672–3, 844–5
  - safety policies 332–5, 428–30, 457–60, 554–8
  - security policies 495, 496–501, 520–3, 554–8, 661–6, 839–43, 849
  - system access controls 576–9, 661–6
- political/country risks 368
- 'polluter pays' principle 464–5
- pollution 332–8, 463–75
- portable buildings 111
- Portugal 753–4, 822
- post-implementation reviews 549–53
- pre-approval requirements, non-audit services 164, 166
- pre-emptive category of control, concepts 138
- premises, security 272–4, 332–5, 428–30, 453–62
- preventive category of control 137–8, 144, 168–70
- PRF *see* profit-related pay schemes
- pricing and discount policies 8, 286–9, 304–6, 308–13, 343, 345–81, 389–92, 438–42, 714
- see also* product/project accounting
- concepts 353–5, 356–9
  - control objectives 354
  - definition 353
  - risk/control questions 354–5, 357
- prior research 11–12
- Privacy Rights Clearinghouse 673, 679, 682–3
- privatised industries 109
- probabilities, risk 52–3, 54–6, 101–15, 122–3
- problem identification/solving techniques, quality assurance systems 183–4
- procedures 9, 31–2, 49, 123–4, 290, 299–302, 489–501
- see also* policies
- back-up and media management 563–5, 846
  - tendering 9, 290, 299–302
- processes 131–5, 224–35, 559–61, 621–6, 837
- see also* business...; efficiency...
- data protection 621–6
  - definition 837
  - operational auditing evaluations 224–35
  - systems concepts 131–5
- processing IT operations
- concepts 559–61
  - control objectives 559
  - risk/control questions 560–1
- procurement 6, 7–8, 11, 22–3, 42, 285–316, 714, 723
- see also* contracting; purchasing
- product designs, concepts 345–8, 438–42, 473
- product development
- see also* marketing...; research and development
- concepts 8, 343, 345–8, 366, 438–42, 473, 714, 715
  - control objectives 345–6, 438–9

- definition 345, 438
- risk/control questions 346–8, 440–2
- product life business process, concepts 35
- product/project accounting
  - see also* pricing and discount policies
  - concepts 7, 240, 268–70, 353, 447–50, 713
  - control objectives 268
  - risk/control questions 269–70
- production/conversion business process, concepts 33–4
- production/manufacturing 3, 5–6, 8, 12–14, 27–8, 32, 33–4, 42–3, 195–8, 317–42, 385–8, 393–5, 398, 442, 463–75, 714, 723–4
  - see also* facilities...; maintenance; materials...; personnel; planning...; safe...
  - concepts 8, 317–42, 442, 714, 723–4
  - control objectives 318–42
  - definition 317–18
  - environmental issues 8, 318, 335–8
  - law and regulatory compliance 8, 318, 338–9
  - overview of functions 8, 318
  - risk/control questions 319–42
  - SAPG 714, 723–4
- proficiency requirements on auditors 16–18
- profit and loss accounts 54, 67–74
- profit-related pay schemes (PRP) 415–22
- profitability contributions of operational auditing 219–35
- profits warnings 91–4
- project appraisal and monitoring 8, 437, 442–5, 447, 651–4, 715
  - concepts 442–5
  - control objectives 442–3
  - definition 442
  - risk/control questions 443–5
- promotion and advertising
  - see also* marketing...
  - concepts 8, 343, 347, 349, 350–3, 369–71, 391–2, 714
  - control objectives 350–1
  - definition 350
  - risk/control questions 352–3, 391–2
- protective marking schemes (PMS) 497, 503, 506–7, 516–23, 556–8, 640, 850
- Protiviti's website 218
- Public Company Accounting Oversight Board (PCAOB) 120–2, 155–77
  - see also* Sarbanes-Oxley Act 2002
- Public Records Acts 526, 533
- public sector 192, 542, 610–12, 627–35, 681, 763–834, 848–9, 850
- publication schemes 536–41, 628–35, 848–9
- pull/push production activities 195–8
- purchasing 7, 11, 42, 45, 196–8, 246–8, 253–6, 285–316, 433–6
  - see also* accounts payable; creditors; procurement; suppliers
  - concepts 196–8, 285–316
  - control objectives 285–6
  - costs and benefits analysis 286–9
  - JITP 196–8, 285
  - price considerations 286–9, 304–6, 308–13
  - risk/control questions 285, 286–9
- qualifications, recruitment issues 404–7, 663–6, 841–2
- quality assurance systems
  - see also* total quality management
  - concepts 8, 182–7, 214–35, 286–9, 306–10, 314–16, 318, 319–42, 345–81, 469–70, 714, 721
  - control objectives 184–7, 330
  - costs and benefits analysis 183–5, 330–2
  - operational auditing 182–7, 214–35, 330–2
  - production/manufacturing 8, 318, 330–2
  - risk/control questions 185–7, 331–2
  - testing and inspection methods 330–2
- 'quality at source' approaches 195–6
- quality audits, concepts 183–7
- quality circles 195
- quality of information, concepts 14, 57–74, 109, 124–7, 151–77, 850
- quality of products/services 14–24
- quantitative/quasi-quantitative/qualitative performance measures, operational auditing 221–8
- query languages/software 69–74, 613–15
- questions 10, 35–6, 40–74, 148–50, 169–73, 185–7, 208–12, 229–35, 240–75, 285, 286–9, 292–316, 318, 344–81, 384–98, 400, 438, 454, 470, 488, 712–28
  - CSAs 208–12
  - ethics/competencies 148–50
  - finance and accounting 241–75
  - operational auditing evaluations 229–35
  - purchasing 286–9
  - SAPGs 10, 35–6, 40–74, 240–1, 285, 318, 345, 384, 400, 438, 454, 470, 488, 712–28
- R&D *see* research and development
- radical changes 122–3, 178–81
- 'ratio of payroll to other costs', operational auditing evaluations 223–33
- 'ratio of productive/unproductive audit time', operational auditing evaluations 223–33
- re-order levels 380–2, 393–5
- Re-use of Public Sector Information Regulations 2005 526, 646
- recessions 82–3, 219–20
- reconciled input data 67–74, 125–7
- record creation, records management 524–41, 849
- record keeping, records management 524–41, 680–7, 849
- record maintenance, records management 528–41, 849
- record retention, records management 497, 524–41, 562–5, 620–6, 680–7, 849, 851
- recording *see* storage...
- records management (RM)
  - see also* information asset registers; information management
  - best practices 485, 524–41

- records management (RM) (*cont.*)
- concepts 479–88, 496–501, 502–10, 511–13, 515, 517–23, 524–41, 544–5, 646–7, 680–7, 715, 725, 838, 849, 851
  - control objectives 535–6
  - definition 484–5, 524–5, 838
  - digital preservation 531, 532–41, 681–7
  - ISO 15489 484–6, 526
  - legislation 524–41, 646–7, 680–7, 849
  - risk/control questions 536–41
  - types of records 496–7, 502–3, 524–41, 566–9, 622–6, 631–2, 681–2
- recruitment issues 7, 17, 33, 42, 149, 176, 399, 400–10, 439–42, 661–6, 713, 841–2
- auditors 17, 176
  - complaints 406–7
  - concepts 404–10, 439–42, 661–6
  - control objectives 404–5, 664
  - definition 404
  - personnel 33, 42, 149, 400–7, 661–6, 841–2
  - qualifications 404–7, 663–6, 841–2
  - references 404–7, 663–6, 841–2
  - risk/control questions 405–7
  - tests 407
- recycle/reuse/reduce environmental paradigm 463–75
- redundancies 410, 662–6
- reference points, systems concepts 132–5
- references, recruitment issues 404–7, 663–6, 841–2
- registration numbers, VAT 262–3
- registration procedures, quality assurance systems 182–7
- regular transfers with external parties, data transfer types 636–7, 639–44
- Regulation of Investigatory Powers Act 2000 581, 592, 646
- regulations 4–5, 8, 43, 46, 77–9, 96–115, 117–46, 151–77, 202, 242–75, 287–9, 291–316, 319–42, 363–82, 385–98, 400–36, 439–52, 463–75, 479–88, 496–501, 514–41, 602–4, 616–35, 640–7, 674–9, 707–11, 713–15, 721
- see also* legislation; Sarbanes-Oxley Act 2002
- freedom of information 479–88, 497–501, 503–10, 516–23, 525–41, 581–4, 590–1, 627–35, 640–1, 646–7, 763–834, 848
  - list of IT regulations 525–6, 645–7, 729–834
  - records management 524–41, 680–7, 849
- reliability issues 4–5, 88–9, 96–115, 117–46, 170–3, 232, 251–3, 314–16, 493–5, 507–10, 535–41, 556–8, 559–61, 587–9, 595–7, 600–4, 610–26, 651–7, 705–6, 711, 835
- remote operating units
- see also* subsidiaries
  - concepts 276–84, 366–8
- remote working 487, 497–501, 520–3, 585–9, 844
- concepts 585–9, 844
  - control objectives 587–8
  - definition 585–7
  - policies 585–9, 844
  - risk/control questions 588–9
  - statistics 585
- removable media 487, 497–501, 520–3, 533, 566–9, 637–44, 672–3, 844–5
- concepts 566–9, 844–5
  - control objectives 567–8
  - disposals 567–9
  - policies 566–9, 672–3, 844–5
  - risk/control questions 568–9
  - types 497, 566–7, 672–3
- remuneration
- see also* payroll; pension schemes...
  - agents 368–71
  - auditors 176, 233
  - personnel 325–7, 355–62, 400–7, 415–22, 425–7
- renewable energy 464–75
- reporting facilities 67–74, 77–94, 96–115, 117, 124–7, 151–77, 206–7, 226–35, 272–4, 470–5, 673–9, 710–11
- see also* financial information...
- reputations 52–4, 67–74, 91–4, 113, 171–2, 222–35, 296, 330–2, 336–8, 389–92, 468–75, 529–41, 656–60, 675–9
- research and development (R&D) 6, 8, 27, 34, 43, 268, 345, 437–52, 715, 724–5
- see also* product development; project appraisal...
  - concepts 437–52, 715, 724–5
  - control objectives 437–52
  - definition 437
  - development project management 8, 437, 447–50
  - ethics 437
  - grant funding schemes 450–2
  - legal and regulatory issues 8, 437, 450–2
  - overview 437
  - plant and equipment 8, 437, 445–7
  - risk/control questions 437–52
  - SAPG 715, 724–5
  - specialist staff 437–52
  - tests 448–52
- reserves 158–60
- residual risk
- see also* risk...
  - concepts 101–15, 142–3, 208–13
- resourcing considerations, operational auditing 16–19, 30, 170–2, 220–1, 232–5, 289–316, 444–5
- responsibilities 29–30, 47, 87, 100, 112–15, 118–20, 125–30, 135–7, 144, 148–50, 151–77, 195–8, 200–3, 214–35, 265, 369–71, 493–5, 497–501, 518–23, 524–41, 556–8, 563–5, 661–6, 691–3, 851
- agents 369–71
  - audit committees 158–73, 176–7, 211, 214–35
  - business processes 29–30, 118–20, 200–3
  - contracting 291–316, 648–50
  - corporate social responsibilities 16, 21, 91–4, 463–75
  - CSAs 200–2
  - data protection 9, 43–4, 404–7, 479–88, 496–501, 503–10, 514–23, 525–41, 562–5, 581–4, 590–7, 616–26, 631–2, 639–44, 646, 848
  - environmental issues 463–75



- freedom of information 479–88, 497–501, 503–10, 516–23, 525–41, 581–4, 590–1, 627–35, 640–1, 646–7, 763–834, 848
- information asset registers 503, 507–10, 847, 851
- IT 493–5, 497–501, 503, 518–23, 524–41, 556–8, 563–5, 585–9, 601–4, 616–26, 627–44, 645–7, 661–6, 691–3, 851
- JIT 195–8
- joint ventures 280–1
- knowledge management 550–3, 849–50, 851
- list of IT legislation 525, 581, 645–7, 729–834
- Sarbanes-Oxley Act 2002 151–77, 202
- security issues 454–62, 554–8, 661–6, 851
- subsidiaries 276–7
- taxation returns 265
- viruses 691–3, 841, 846
- restatements of prior year results 173
- resurrected deleted files 562, 567, 682–7, 851
- retention
- control objectives 685
  - data retention and disposal 487, 497, 524–41, 562–5, 620–6, 638–44, 680–7, 849, 851
  - personnel 149–50, 325–7, 401–4, 441
  - risk/control questions 685–7
- return on capital employed (ROCE) 194
- returned goods 289, 361–2
- returns 262–3, 264–6, 273–5, 424
- revenue business process, concepts 32–6, 720–8
- revenue expenditure, software assets 502–3
- reviews
- operational auditing 214–35
  - project outturn/performance 313–16
- risk 3–6, 10, 17, 22, 25, 29–30, 36–7, 40, 41–74, 76–94, 95–115, 120–3, 137–9, 148–50, 168–70, 201–13, 453–62, 658–60, 667–70, 671–9
- appetites 95–115, 208–13
  - aversion 111
  - categories 102–6, 113–15, 122–3, 137–9, 168–70, 208–13
  - concepts 40, 45–6, 50–74, 95–115, 120–3, 137–9, 148–50, 168–70
  - control matrices 40, 53–4, 56–74
  - definition 52, 101
  - exposures 52–3, 55–74, 99–115, 453–62
  - levels 51–2, 102–4, 113–15, 143–5
  - matrices 101–6
  - mitigation 101–15, 207–8, 211–12, 453–62, 658–60, 667–70, 671–9
  - owners 107
  - registers 101, 106–8, 115, 168–70
  - responses 95–115, 122–3
  - sponsors 107
- ‘risk assessment’ component, COSO internal control framework 120–1, 122–3, 142, 144, 147–50, 157–8, 163–77
- risk assessments, concepts 51–74, 85–6, 95–115, 120–1, 122–3, 137–9, 148–50, 168–70, 201–13, 215–35, 277–84, 368, 427–30, 453–62, 481–8, 566–9, 658–60, 699–706, 707–9
- risk management 3–6, 10, 17, 22, 25, 29–30, 36–7, 40, 41–74, 75–94, 95–115, 122–3, 137–9, 152–77, 202, 205, 207–8, 232–5, 453–62, 470–5, 481–8, 674–9, 712–13, 718, 721
- see also* Sarbanes-Oxley Act 2002
- activities fan 99–100
  - concealed risks 107–10
  - concepts 75–94, 95–115, 122–3, 137–9, 152–77, 202, 205, 207–8, 453–62, 470–5, 481–8, 674–9, 718, 721
  - control issues 75–94, 96–8, 112–15, 122–3, 232–5
  - corporate governance 76–94, 110
  - definition 95–8
  - essential effective components 98–9, 120–3, 124–8, 142, 144, 147–50
  - internal controls 75–94, 96–8, 112–15, 122–3, 137–42, 147–50, 151–77, 232–5
  - limitations 107–15
  - objectives 77–81, 85–6, 95–8, 112–15, 122–3
  - opportunities 111, 113–15, 226–8
  - organisational cultures 110, 115, 678–9
  - processes 95–115
  - ‘Rubik cube’ 98–9, 120–1
  - SAPG 712, 718
  - scope of internal audit’s role 99, 201–2
  - simultaneous risks 110–11
  - strategic objectives 96–8, 112–15
  - subjective judgements 104
  - tools 101–7
- risk/control section of SAPGs, concepts 45–6, 47–50
- robust systems 36, 141–2, 507–10, 521–3, 587–9
- Romania 754, 823
- Royal Dutch Shell 485–6
- ‘Rubik cube’, risk management 98–9, 120–1
- Russian Federation 280–1, 754, 823
- Rwanda 754, 824
- safe production/manufacturing environment 8, 318, 319, 322–4, 332–5, 339, 413–15, 427–30, 457–60
- safety policies 332–5, 428–30, 457–60, 554–8
- sales 3, 5–6, 8, 27–8, 32–5, 43, 51, 113, 136, 194, 343–82, 385–8, 393–5
- see also* marketing...; order processing
- quotas 356–9
- sales management 8, 343, 355–62, 442, 714
- concepts 355–62, 442
  - control objectives 356
  - costs and benefits analysis 360–2
  - definition 355–6
  - remuneration 355–62
  - risk/control questions 357–9
- sales performance and monitoring 8, 343, 346, 359–62, 714
- concepts 359–62
  - control objectives 360
  - definition 359
- sales tax *see* VAT
- samples 168–70
- SAP, IBM 199

SAPGs *see* standard audit programme guides

Sarbanes-Oxley Act 2002

*see also* internal controls; Public Company Accounting Oversight Board

breaches 152–4

complacency dangers 167–8

concepts 151–77, 202

control registers 168–70, 173

COSO internal control framework 157–77

costs and benefits analysis 151, 154–5, 171–2

criminal sanctions 152–4, 164–77

documentation requirements 167–70

overview of sections 151–4

recognised suitable control frameworks 157–8

s.101 166

s.201 (Services Outside the Scope of Practice of Auditors) 152, 164, 166–7

s.206 (Conflicts of Interest) 152, 163–4

s.301 (Public Company Audit Committees) 152, 158–60, 176

s.302 (Corporate Responsibility for Financial Statements) 151, 153, 156–77, 202

s.303 (Improper Influence on Conduct of Audits) 152, 164–5

s.404 (Management Assessment of Internal Controls) 117, 141–2, 151–77, 202

s.406 (Code of Ethics for Senior Financial Officers) 152, 161–3

s.407 (Disclosure of Audit Committee Financial Expert) 152, 158, 161

s.906 (Corporate Responsibility for Financial Statements) 152–4

SOX-Lite 155–6

standardisation incentives 170

Saudi Arabia 755, 824

scientific management 198

SCL 560–1, 575

scope of operational auditing 3–12, 16–17, 27–39, 152, 164, 166–7, 170–3, 201–2, 218–35, 239–40, 469–75, 707–9

screensavers 623

SD memory cards 566–7

Securities & Exchange Commission (SEC) 117, 120, 141–2, 151, 154–77

Securities Exchange Act 1934 152–4, 157–77

security 272–4, 332–5, 428–30, 453–62, 463–75, 481–8, 489–95, 504–10, 514–23, 527–41, 554–8, 576–9, 613–15, 636–44, 651–7, 671–9, 713, 721, 836, 839–51

*see also* access...; health and safety; insurance...

contingency plans 43–4, 69–74, 91, 103, 368, 397–8, 453–62, 497–501, 512–13, 528–41, 561, 658–60, 671–9, 707–9

control objectives 454–62, 664

data protection 9, 43–4, 404–7, 479–88, 496–501, 503–10, 514–23, 525–41, 562–5, 581–4, 590–7, 616–26, 631–2, 639–44, 646, 729–62, 848

data retention and disposal 487, 497, 524–41, 562–5, 620–6, 638–44, 680–7, 851

definition 453–4

fire hazards 332–5, 428–30, 454–62, 554–8, 660

information asset registers 504–10, 847

information security incidents 487, 520–3, 671–9, 681–3, 707–9, 841–2

IT health checks 487, 707–9

IT sites and infrastructure 486, 487, 520–3, 554–8, 658–60, 671–9, 681–7, 843

logging systems 487, 576–9, 588–9, 667–70

overview 454

passwords 58–74, 518–23, 527–41, 576–9, 585–9, 601–4, 623–6, 638–44, 707–9, 843

policies 495, 496–501, 520–3, 554–8, 661–6, 839–43, 849

records management 527–41, 849

removable media 487, 497–501, 520–3, 533, 566–9, 672–3, 844–5

responsibilities 454–62, 554–8, 661–6, 851

risk/control questions 454–62, 665–6

spreadsheets 699–705

system access controls 8, 487, 576–9, 661–6, 667–70, 707–9

Security Industry Authority (SIA) 555

security services 555–8

selection and letting of contracts, concepts 9, 290, 304–6

self-actualisation concepts 190–1

sensitive company data 57–74, 124–7, 220–1, 242, 272–4, 299–302, 345–8, 351–5, 401–7, 438–42, 453–62, 503–10, 515–23, 533–41, 560–1, 566–9, 586–9, 592–7, 616–26, 636–44, 663–6, 671–9, 680–7, 688–90, 700–6, 729–62, 838

*see also* data protection

sensitive data, data protection 617–26, 636–44, 646, 729–62, 848

'seq' column of SAPG risk/control section 48–50

Serbia 755, 824

servers 487, 548, 554–8

service level agreements, IT 493–5

service packs/releases 571–5

service provisions 5–6

share option schemes, personnel 415–22

share prices 93

share schemes, personnel 415–22

shareholders 81–2, 90–4, 97–8, 128–9, 464, 473–5

*see also* corporate governance; stakeholders

sharing aspects of information management 515–23, 542–53, 636–44

ship analogy, internal controls 119–20

shredders 683–4

'significant deficiencies', definitions 153, 156–7, 172

'significant misstatement', definitions 153, 156–7

signing-off procedures 49

simultaneous risks, risk management 110–11

Singapore 755, 825

sites and infrastructure for IT

*see also* physical security

concepts 486, 554–8, 715, 725, 843

'size' row in control matrices 58–74

- skills 16–18, 84–90, 122, 148–50, 158–60, 204–5, 218, 233–4, 241–2, 294–5, 318–27, 337–42, 351–66, 385–8, 396–8, 400–4, 408–13, 439–42, 489–95, 559–75, 651–4, 684
- Skills for Security 684
- Slovakia 756, 825
- Slovenia 756, 825
- software 9, 43–4, 64, 67–74, 487, 489–92, 511–13, 520–3, 531–41, 559–61, 570–5, 585–9, 605–8, 648–50, 651–7, 691–3, 699–706, 845
- concepts 502–10, 554–8, 655–7, 691–3, 845
- malicious software 9, 43, 497–501, 520–3, 563–9, 570–5, 583–4, 590–7, 601–4, 671–9, 691–3, 707–9, 841, 846
- processing IT operations 559–61
- selection considerations 655–7, 845
- systems and operating software 9, 43–4, 64, 71–4, 487, 559–61, 570–5, 667–70
- software maintenance/development controls 9, 43–4, 64, 67–74, 487, 605–8, 651–7, 699–706, 845
- concepts 605–8, 651–7, 845
- control objectives 606–7
- risk/control questions 607–8
- South Africa 140, 141, 756, 826
- South Korea 757, 826
- SOX *see* Sarbanes-Oxley Act 2002
- SOX-Lite, concepts 155–6
- Spain 757, 827
- spam 590–7, 602, 707–9
- span of control, concepts 118–20, 187–8
- spare parts and supply 8, 343, 380–2, 715
- concepts 8, 343, 380–2
- control objectives 380–1
- risk/control questions 381–2
- specialisation 135–7, 142–3
- specialist staff, research and development 437–52
- specifications, system development 651–7, 706
- sponsors 4–5, 15, 75–81, 96–9, 103, 107, 111, 115, 117–28, 140, 142, 144, 147–50, 157–77, 351–3
- spreadsheets 40, 53–4, 56–74, 487, 699–706
- access controls 704–6
- concepts 70, 699–706
- control matrices 40, 53–4, 56–74
- control objectives 705
- documentation needs 701–6
- error types 699–700, 702
- good practice 70, 699–706
- ICAEW best practices 70
- inventories 700–1
- risk assessments 699–706
- risk/control questions 706
- tests 705–6
- spyware 570–5, 596–7, 601–4, 672–9
- staff appraisals 7, 234, 314–16, 324–7, 399, 400–4, 413, 424–7, 713
- concepts 424–7
- control objectives 425
- risk/control questions 425–7
- stakeholders 22, 75–82, 90–4, 112–15, 464–75
- added value definition 22
- corporate governance 75–82, 90–4
- environmental issues 464–75
- types 91
- standard audit programme guides (SAPGs)
- see also* control self assessments
- concepts 10, 35–6, 40–74, 240–1, 285, 318, 345, 384, 400, 438, 454, 470, 488, 712–28
- examples 41–5
- format proposals 45–51
- index 712–28
- objectives section 46–7
- practical uses 41–5, 240–1
- purposes 46, 240–1, 719–21
- questions 10, 35–6, 40–74, 240–1, 285, 318, 345, 384, 400, 438, 454, 470, 488, 712–28
- risk/control section 45–6, 47–50
- system interface section 46, 50
- title page section 46–7
- standard cost variances 268–70, 711
- standards 3, 11–12, 16–19, 21–6, 76–80, 95–8, 115, 121–2, 139–5, 139–41, 171, 176, 182, 183–4, 214–17, 225, 229, 232–5, 272–5, 276–84, 287–9, 295–7, 319–42, 400–36, 465–75, 480–8, 515–41, 554–8, 652–4, 707–9
- see also* British Standards...; ISO...
- data retention and disposal 684–5
- data transfers and sharing 515–23, 542–53, 636–44
- emails 593–7
- environmental auditing 465–75
- financial information and reporting 272–4, 710–11
- IIA 3, 11–12, 16–19, 21–6, 76–80, 95–8, 115, 121–2, 139–41, 171, 176, 214–17, 225, 229, 232–5, 570
- IT 480–8, 493–5, 515–41, 581–4, 645–7, 652–4, 701–6
- systems concepts 130–5
- stock control
- concepts 7–8, 380–2, 392–5, 398, 714
- control objectives 392–3
- risk/control questions 393–5
- stock and materials handling 6, 7–8, 11, 33–4, 42, 45, 51, 195–8, 240, 266–8, 321, 327, 362–6, 380–2, 383–98, 714, 723
- see also* inventories; spare parts...
- concepts 7–8, 383–98, 714, 723
- out-of-stock situations 380–2, 392–5
- overview 383–4
- re-order levels 380–2, 393–5
- SAPG 714, 723
- storage aspects of information management 515–23, 544–53, 563–5, 586–9, 844–5
- see also* removable media
- strategic objectives 96–8, 112–15, 178–81, 281–4, 291–316, 345–81, 388–92, 402–36, 438–52
- environmental issues 467–8

- strategic objectives (*cont.*)  
   risk management 96–8, 112–15
- strategic planning  
   concepts 8, 71–4, 281–4, 291–316, 345–81, 438–42, 486, 489–92, 511–13, 582–4, 715, 725  
   IT 8, 486, 489–92, 511–13, 582–4, 715, 725
- strengths and weaknesses analysis 71–4
- subjective judgements, risk management 104
- subsidiaries 3, 265, 276–84, 366–8  
   *see also* parent companies; remote operating units  
   concepts 276–84, 366–8  
   cultural issues 277–84, 366–8  
   fact-finding programmes 277–8  
   marketing and sales 366–8  
   responsibilities 276–7  
   taxation 265, 366–8
- ‘substantive testing’ column of SAPG risk/control section 48–50, 56
- succession planning, concepts 7, 399, 407, 408–10
- Sudan 757, 827
- suppliers 33–4, 91–4, 194–8, 286–316, 655–7  
   *see also* purchasing
- supply chains, environmental issues 468–75
- sustainability reports 470–5
- Sweden 627, 757–8, 828
- Switzerland 758, 828
- synergy 344, 469–75
- system access controls  
   *see also* access controls  
   concepts 8, 487, 576–9, 642, 661–6, 667–70, 707–9, 837  
   control objectives 577  
   definition 576, 837  
   risk/control questions 578–9
- system administrators 576–9, 838
- system development 487, 651–7, 699–706, 845  
   concepts 651–7, 699–706, 845  
   control objectives 651–2, 655–705  
   costs and benefits analysis 651–4  
   risk/control questions 652–4, 656–7, 706  
   sourcing considerations 651, 655–7  
   spreadsheets 699–706  
   tests 652–7
- system interface section of SAPGs 46, 50–1
- system risk  
   *see also* risk  
   definition 52–3
- systems concepts 130–5, 719–20
- systems and operating software 8, 43–4, 64, 71–4, 487, 559–61, 570–5, 667–70  
   concepts 570–5, 667–70  
   control objectives 573–4  
   definition 570–1  
   risk/control questions 574–5  
   updates 570–5, 584
- table PCs 585
- tacit knowledge  
   *see also* knowledge...
- concepts 544–53, 838
- tactical level of risk, concepts 51–2
- Taiwan 758, 829
- taxation 7, 33, 42, 51, 53–4, 91, 164, 166, 240, 244–5, 246–51, 261–6, 269, 311, 312, 354–5, 366–8, 416–24, 434–6, 442, 517–23, 713, 722  
   allowances 264–6  
   concepts 261–6, 311–12  
   control objectives 262, 264, 311–12  
   parent companies 366–8  
   returns 262–3, 264–6  
   risk/control questions 262–3, 264–6, 311–12  
   VAT 7, 51, 240, 246–51, 255–6, 261–3, 271–2, 312, 355, 713, 722
- Taylor, Frederick 195, 198
- TCP/IP 598, 707
- teams 183–7, 200–1, 204–12  
   *see also* personnel
- technical activities, resourcing considerations 16–19
- Telecommunications Regulations 2000 526, 646
- telephones 28, 609, 840–1
- temporary/short-term staff 403, 409, 576–9
- tendering 7, 9, 22–3, 44, 191–5, 220–1, 290–316, 651–4, 716–17, 726–8  
   *see also* contracting  
   concepts 9, 290, 299–304  
   control objectives 299–300, 302–3  
   definition 299  
   documentation 300–1, 302–5  
   procedures 9, 290, 299–302  
   risk/control questions 300–2, 303–4
- termination of employment 400–4, 410, 425–7, 662–6, 841–2
- termination/contingency plan options, risk matrices 102–6
- terms of reference, IT function 493–5
- ‘test’ row in control matrices 58–74
- test scripts, concepts 169–70
- tests 14, 48–74, 125–7, 167, 168–73, 194–5, 330–2, 347–8, 442, 448–52, 652–60, 689–90, 705–6, 707–9  
   concepts 168–73, 330–2, 347–8, 652–60, 689–90, 705–6, 707–9  
   contingency plans 658–60, 689–90  
   EDI 689–90  
   information flows 14, 125–7, 167, 168–73, 689–90  
   IT health checks 707–9  
   production/manufacturing quality controls 330–2  
   R&D 448–52  
   recruitment issues 407  
   spreadsheets 705–6  
   system development 652–7
- Thailand 758, 829–30
- three Es of effectiveness, efficiency, and economy, concepts 15–16, 19–21, 29–30, 77–9, 84, 85, 117–46, 215–35
- three Es of equity, environment, and ethics, concepts 16, 21, 84–5, 463–75
- time business process, concepts 35

- time divisions, internal controls 137, 227–8
- timeliness of reports 272–4, 283, 289, 291–316, 448–50, 514–23, 559–61, 710–11
- timings, development project management 447–50
- title page section of SAPGs 46–7
- TJX Companies Inc. 672–3
- Tokyo Stock Exchange 106
- total quality management (TQM)  
*see also* continuous improvements; quality...  
 concepts 178, 181–7, 330, 469–70  
 costs and benefits analysis 183–5  
 definition 181  
 risk/control questions 185–7
- Towers, Stephen 180–1
- Toyota 195
- TQM *see* total quality management
- trade marks, distributors 366, 392
- trades unions 91, 427, 431–2
- training and development 7, 15–17, 64, 71–4, 90, 138, 144, 149, 204–5, 212, 218, 234, 241–2, 294–5, 314–16, 319–22, 324–7, 337, 339–42, 351–66, 370, 396–8, 399, 400–4, 408–13, 439–42, 448–50, 489–501, 518–23, 536–53, 572–5, 614–15, 657, 661–6, 699–706, 713  
 concepts 410–13, 439–42, 448–50, 699–706  
 control objectives 410–11  
 costs and benefits analysis 411–13  
 definition 410  
 IT 489–92, 518–23, 536–53, 572–5, 583–4, 657, 661–6, 699–706  
 knowledge management 542–53  
 risk/control questions 411–13
- transparency issues 85–6, 91–4, 516–23, 628–35
- transport 8, 383, 384–8, 714  
*see also* distribution
- Treadway Report 118, 157  
*see also* Committee of Sponsoring Organizations
- treasury  
 concepts 7, 33–4, 36, 51, 240–3, 713, 720–8  
 control objectives 241  
 risk/control questions 241–3
- trends 16
- Trinidad and Tobago 758, 830–1
- ‘triple bottom line’ objectives 464, 473
- Trojans 672, 691–3
- trust levels, CSAs 209–13
- Turkey 759, 831
- Turnbull internal control framework 117–18, 120, 128–9, 140–2, 144, 157–8, 170–1  
*see also* UK, Combined Code on Corporate Governance
- turnover rates, personnel 149–50, 325–7, 401–4
- ‘type’ row in control matrices 58–74
- Uganda 759, 831
- UK 22–3, 109, 117–18, 120, 128–9, 140, 144, 157–8, 170–1, 176–7, 218–19, 245, 464, 466, 526, 533–5, 555, 581, 585–9, 590–2, 599, 609–10, 616–35, 658, 671–9, 681, 684–5, 759–60, 832–3
- Combined Code on Corporate Governance 128–9, 140, 144, 157–8, 170–1, 176–7
- Companies Act 2006 464, 473–5
- Department of Trade and Industry 480
- HM Treasury 218–19
- Ukraine 759, 831–2
- United States Code (USC) 154
- university case study, cycles 37–9
- untrue statements 151–77
- up-to-date information  
 data protection 619–26, 848  
 information management 514–23, 619–26
- updates  
 access rights 662–6  
 systems and operating software 570–5, 584
- Uruguay 761, 833–4
- US 117–28, 151–77, 465–6, 534–5, 581, 627, 671–3, 682–3, 684–5, 760–1, 833  
*see also* Committee of Sponsoring Organizations; Sarbanes-Oxley Act 2002
- Environmental Protection Agency 465–6
- USB memory sticks 566–7, 637
- users  
 screening processes 662–6, 667–70, 694–5  
 support services 487, 694–5
- utilisation aspects of information management 515–23, 544–53
- Uzbekistan 834
- validation tasks 13–14, 241–75, 291–316, 405–7, 698, 702–6, 710–11
- valuations  
 interim payments 9, 44, 290, 308–10  
 inventories 266–8
- value for money auditing (VFM), concepts 21–3, 230–3, 353
- values 16, 34, 78, 84–5, 121–2
- variables, systems concepts 131–5
- variances 268–70, 278, 382, 395, 711
- VAT 7, 51, 240, 246–51, 255–6, 261–3, 271–2, 312, 355, 713, 722  
 control objectives 262  
 registration numbers 262–3  
 returns 262–3  
 risk/control questions 262–3, 312
- VBA 703
- Venezuela 761, 834
- verification tasks 13–14, 241–75, 291–316, 405–7, 468–75, 576–9, 662–6, 698, 702–6
- versions of software 571–5
- vertical integration 194
- VFM *see* value for money auditing
- viability/competence assessments of contractors, concepts 9, 290, 295–7
- Vietnam 762, 834
- virtual private networks (VPNs) 585–9, 609–12
- viruses 9, 43, 487, 497–501, 520–3, 563–9, 570–5, 583–4, 590–7, 601–4, 671–9, 691–3, 707–9, 841, 846

- viruses (*cont.*)  
  concepts 691–3, 846  
  control objectives 691–2  
  emails 691–3, 841  
  risk/control questions 692–3  
vision 209–13  
Voice over IP telephony (VoIP) 609
- walkthrough tests 168–70  
WANs *see* wide area networks  
warehousing and storage 7–8, 42, 51, 327, 383–4,  
  395–8, 714  
  *see also* distribution; stock...  
  concepts 395–8  
  control objectives 396  
  definition 395  
  risk/control questions 396–8  
warranty arrangements 8, 43, 51, 343, 375–7, 381–2,  
  714  
  *see also* after sales support  
  concepts 8, 43, 51, 343, 375–7, 381–2  
  control objectives 375–6  
  risk/control questions 376–7  
waste management 335–8, 463–75  
‘weakness to report’ column of SAPG risk/control  
  section 48–50  
websites 10, 35–6, 40, 44, 92–3, 218, 712, 729–834
- Weinstock, Lord 97–8  
welfare of personnel 7, 399, 400–4, 413–15, 457–60,  
  555–8, 713  
  *see also* health and safety at work; security  
  concepts 413–15, 457–60, 555–8  
  control objectives 413  
whistleblowing policies 84–5, 121–2, 149  
why-what-who-how questions, knowledge management  
  549–50  
wide area networks (WANs) 489, 609–12, 693  
Wiley website 10, 35–6, 40, 44, 712  
Windows 570–1  
Word tables 206  
working capital 242–3  
workshop/survey approaches to CSA 200–1, 204–12  
worms 672  
‘WP’ (working paper) column of SAPG risk/control  
  section 48–50
- Yemen 762, 834
- Zimbabwe 762, 834