## Index

### Symbols

- 80/20 execution strategy 195, 202–203
- **A**
  - access
    - control mechanisms 285–300
    - combination frameworks 286–287
    - extensible access control markup language (XACML) 286–287
    - Tivoli policy director 286–287
    - delegation frameworks 287–290
    - KeyNote 287
    - PolicyMaker 287
    - role-based trust management (RT) framework 287–288
    - evaluation 288–289
    - state 286
  - management 210, 228–234
  - auditing 233–234
  - audit logs 233–234
    - entitlement review audits 233
    - entitlements log 234
    - security change audits 233
    - security changes log 234
    - violation audits 233
    - violation logs 234
    - authentication 229–230
  - biometrics 230
  - digital certificates 230
  - factors 229
  - Kerberos 229–230
  - security tokens 230
  - authorization 230–231
  - major concepts 210
  - role based access control (RBAC) 231–232
    - benefits 231
  - single sign on (SSO) 232–233
  - systems 191
  - advanced measurement approach (AMA) 122
  - Anti-Phishing Working Group 243, 246
  - antivirus programs 16
  - asset and liability management (ALM) activities 30
  - authentication 154–164
    - concept 154
    - evaluation criteria
      - accessibility across different interaction channels 163
      - ease of use 162–163
      - flexibility 163
      - scalability and cost effectiveness 163
      - security 163
    - factors 154–155

---

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
in an electronic banking environment 160
legal considerations
  customer service agreements 163–164
  licensing 163
  privacy policies 164
  variable risks 164
authorization
  request cryptogram (ARQC) 184
  response cryptogram (ARPC) 184
automated
clearing house (ACH) 63
provisioning
  benefits 223
teller machines (ATMs) 64, 153, 187
  networks 64
  systems 62
avoidance 5, 11
awareness 5

B

bank
  Bank Secrecy Act (BSA) 68
  information 61
Basel II Accord 31, 39, 42, 50, 54, 267
  Revised International Capital Framework 201
behavioral score cards 265
best practice 54
biometrics 67–68, 156
  authentication schemes 139
  fingerprint verification 156
  retinal and iris scanning 156
  voice verification 156
bot programs 243
brand spoofing. See phishing
business
  impact analysis (BIA) 85
  intelligence (BI) 204
    systems
      analysis 279
      technology
context handling 278–280

C

California Information Practices Act (SB 1386) 3, 201, 314
CAMEL ratings 77
Canadian Privacy Act, Chapter P-21 202
carding. See phishing
certified policy (CP) frameworks 290–299
enforcement 292
  primitive operations 293–295
  certificate operations 293–294
  communication primitives 295
  control-state operations 294
  subscription term expression 293
  system architecture 291–292
chief
  credit officer (CCO) 33
  identity officers (CIOs) 192
  information officer (CIO) 192
  security officer (CISO) 192
  risk officer (CRO) 33
  cluster servers 299–300
comprehensive analysis: 102
core banking system 62
control objectives for information and related technology (COBIT) 203
cryptography 182
coprocessors 169, 174, 186
core banking system 62
cost-benefit analysis (CBA) 9, 102
critical infrastructures (CI) 310, 312
credit risk 103
  29
cyber crime 242–258
cybernetics 93, 101, 107, 110

data
  assurance 272–274
**Index**

definition 277  
protection 12–13  
dedicated lines 65  
defense-in-depth 12  
methodology 79–80  
people 79  
processes 79–80  
technology 80  
strategy 15–16  
structure 10  
definition risk 28  
denial-of-service (DoS) attacks 209, 243  
deprovisioning 224–225  
detection 13  
deterrence 5, 11–12, 21  
digital signatures 137  
directories 217–218  
services 218  
duration gap analysis 35  
dynamic data authentication (DDA) 184

**E**

electronic  
banking (e-banking) 137–150  
authentication  
evaluation 141–146  
security goals  
confidentiality 139  
integrity 139  
mutual authentication 139  
non-repudiation 139  
tamper resistance 140  
usable security 140  
user authentication 139  
commerce (e-commerce)  
security 93–95  
definition 93  
information security 94–95  
physical security 94  
funds transfer (EFT) 63  
association (EFTA) 72  
enforcement 5, 21  
enterprise  
identity stack rationalization 192–193  
information architecture (EIA) 192  
environmental risk 28–29

Europay, Mastercard, and Visa (EMV)  
cards 182–187  
European Union DataPrivacy Directive (EUDPD) 201  
extpert forecast 102  
extensible access control markup language (XACML) 231

**F**

Federal  
Financial Institutions Examination Council (FFIEC) 66, 153, 160  
Trade Commission (FTC) 2  
feedback method 109  
financial  
information 61  
institution fraud  
counterfeiting 182  
scimming 182  
risk 28–29  
Services Information Sharing and Analysis Center (FS/ISAC) 312  
firewalls 15, 16, 65  
flow chart analysis 102  
fraud 262–281  
detection 263–272  
artificial intelligence 264–272  
intelligent analysis engines 268  
unsupervised neural networks 266–267  
social network analysis 270–272  
external threats 266  
intelligence systems 278–280  
internal threats 266–267  
"opportunity makers" 267  
"opportunity takers" 267  
detection 268  
prevention 264  
funds-transfer system 62

**G**

Glass-Steagall Act 68  
globally unique identifier (GUID) 196  
Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) 3, 5, 68, 201, 211, 213, 233, 310, 314

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
hardware-based authentication 138–139

cryptographic hardware tokens 137, 140, 154

GSM mobile phones 137–141, 145, 147

SIM cards 138

password generators 154–155

ActivCard 137–147

SecurID 138

security modules (HSMs) 160

Health Insurance Portability and Accountability Act 1996 (HIPAA) 201

Hong Kong Personal Data Privacy Act 202

identity

aggregation 219–222

and access management (IAM) 16, 191–206, 209–238

benefits 205–206

compliance audits 200

goals 209–210

implementation 235–236

risks 205

standing committee 194

consolidation 218–219

criteria 219

data

mastering 196–197

provisioning 197–198

rationalization 196

definition 211

fraud 69, 262

management 210, 211–228

lifecycle 211–213

audit 212–213

creation 212

deletion 212–213

maintenance 212–213

utilization 212

major concepts 210

systems 191

rationalization 193–194

stores 213–214, 216

synchronization 219–222

theft 70, 153, 243, 248

information

assurance (IA) 274–276, 281

alignment 47–48

dilemmas 56–57

process 48, 50–54

management 285–300

strategy 46–57

definition 277

method 109

security 60–87, 104

strategy

evolution 95–96

security programs (ISPs) 83–86

auditing 86

business continuity planning (BCP) 85

incident response 86

risk assessment program 83–84

security awareness testing 84

social engineering testing 84

vulnerability and penetration testing 84

sharing and analysis centers (ISACs) 312

system audit (ISA) 98

technology audit (IT audit) 98

Information Technology Governance Institute (ITGI) 203

insider attacks 159

internal

control 54

rate of return (IRR) 9

Internet banking 62–63

intrusion

detection systems (IDSs) 13, 16, 65

prevention systems (IPSs) 13, 14, 16

K

keylogging programs 67, 243

Ki 179, 184

L

layered authentication 161

lightweight directory access protocol (LDAP) 216, 218, 238
liquidity risk 29
local area network (LAN) 64

M
man-in-the-middle attacks 159
metadirectories 220, 238
microcontroller devices 169–173
microprocessor chips 168
money laundering 72–73, 262, 265
multifactor authentication 67, 229

N
net present value (NPV) 9
networks 62, 64–65
New Basel Capital Adequacy Standards 103–104, 112, 132

O
one-factor authentication 67
one-time passwords 67
OpenLDAP 217
operational risk 28–29, 31, 32
out-of-band authentication 157–159
outsourcing 65–66

P
passwords 137, 145, 154
management 227–229
password complexity 227–228
password policy 227
self-service 228
personal identification number (PIN) codes 138–139, 149, 184–185, 229, 249
pharming 70–71, 159, 243, 245, 247–248
definition 247
phishing 70–71, 153, 159, 242–258, 262
attacks
data theft 246
deoceptive phishing 246
Spear phishing 246
Hosts file poisoning 246
keyloggers 246
malware-based phishing 246
session hijacking 246
web Trojans 246
business response 249–250
definition 245
history 245
legal response 250
Anti-Phishing Act of 2005 252
California Anti-Phishing Bill 250–251
Convention on Cybercrime 254–256, 258
Identity Theft Penalty Enhancement Act (ITPEA) 253
Revised UK Fraud Bill 253–254
preventative measures 257
prevention 12
privacy 6
probability of default (PD) 285
probing attacks 306
product market risk 30
provisioning 222–224
HR provisioning 224–225
Self-service provisioning 224
software 238
workflow 225–226

R
reconstruction 15
recoverability 14
regulatory agencies 73–77
Board of Governors of the Federal Reserve 74
Federal Deposit Insurance Corporation (FDIC) 75
Federal Financial Institutions Examination Council (FIEC) 73–74
National Credit Union Administration (NCUA) 76–77
Office of the Comptroller of the Currency (OCC) 75
Office of Thrift Supervision (OTS) 76
regulatory compliance 200
IAM Strategies 200
remote access Trojans (Rat-ing) 243, 245, 247
definition 247
resiliency 14
restoration 14–15

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
return on
critical infrastructure protection investment (ROCIPI) 25
cyber security investment (ROCSI) 25
investment (ROI) 9
privacy investment (ROPI) 5
security investment (ROSI) 5, 203
risk
-risk-based management 80–83
-tree analysis 101
analysis 8–11
benefit analysis 102
control 114, 118–119
evaluation 114, 116–118
identification 34, 114–116
methods
(accident tree analysis (ATA) 115
risk survey and analysis table 115
management 27–43
activities 31
feedback
(auditing 119
monitoring 119
improvement 122–124
process 30
management life cycle 81
trade-off analysis 102
roles based access management (RABM) 198–200
S
Sarbanes-Oxley Act (SOX) 3, 50, 54, 6
8, 201, 211, 213, 233, 262, 267, 305–314
and intellectual property (IP) 311
benefits 307
compliance 306
costs 306
section 302 305
section 404 305–310
screening monitor diagnostic 102
sector
-specific agencies (SSAs) 312
coordinating councils (SCCs) 312
secured memory 168
secure socket layer (SSL) 139
Securities and Exchange Commission (SEC) 3
security
-breach 2, 4–6, 6–7, 23–24
definition
  confidentiality + integrity + availability (CIA) 5
expenditures 3
forums 55
measures 2, 3
portfolios 17–18
risk management 93–133
implementation
  feedback 127–134
  IT solutions 124–126
management solutions 126–127
standards and regulations 97–98
strategy 106–107, 111
theory 96–97
risks 113
tokens 168
service level agreement (SLA) 66
services oriented architecture (SOA) 191
simple power analysis (SPA) 179
single-factor authentication 155
SiteKey 154
skimming 71–72
smart
cards 154, 156–157
-attacks
  fault 181
  logical 176–177
  physical 176–179
  side-channel 176, 179–181
chips
  general features 170
contact cards 172
contactless cards 172–173
life cycle management system (SCLC-MS) 186
management system (SCMS) 187
operating systems (SCOS) 173
GlobalPlatform 173, 175
Java Card 173–175
Java Card and GlobalPlatform (JCGP) 173
Multos 173–174
Windows for smart cards (WfSC) 173
pin outs 170–171
readers 182
system 167–187
terminal devices 170
tokens 157
software-based authentication 138–140
signature files 141–142
SSO software 238
standardized directory services 196–198
statement of auditing standards (SAS) 67
static data authentication (SDA) 183
statistical appraisal analysis 103
subscriptions 285, 288
updates 296–299
suspicious activity report (SAR) 73
system
environment adaptability 108
integrity 108
order 108
purpose 108
relevance 108
systematics 93, 101, 107–113
theory 112

T
'three Vs' of profiling
value 265
velocity (timing) 265
volume 265
tamper resistance 168–169
targeted scans 306
technology integration 65
The Financial Services Modernization Act of 1999. See Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
tokens 67
total cost of ownership (TCO) 162
acquisition costs 162
deployment costs 162
ongoing costs 162
Trojan horse attacks 137, 159
trust 147–150
two-factor authentication 139, 154

U
unified
access management 198–199
strategies 198
application management 204
business process alignment 203–204
enterprise correspondence 204
identity and access management framework 200
uniform
rating system for information technology (URSIT) 78
user account proliferation 213–214
reasons 214

V
value-at-risk (VaR) 35, 102
virtual directories 220
viruses 17
VPNs 65

W
wide area network (WAN) 64
worms 17

Z
zombie network 248