Index

Boldface numbers indicate illustrations and tables.

A

Access control, 1, 36-38, 57, 81, 86, 108, 154, 156-157
- in academia, 198
- attribute-based (ABAC), 61-**62**, 65-69, **66**, 75-76, 82-83
- authentication and, 44, 47
- authorization and, 7
- CIO's role in, 16
- cloud and, 1, 30, 174, 234
- data sharing and, 169, 173, 177
- dynamic, 11, 234
- fingerprint recognition for, 232
- in health care, 197-198, 227
- hierarchy, **26**
- in IAM, 19-20
- industrial computer systems and, 164-166
- Internet of Things and, 1, 13
- OAuth and, 31, 123
- policy, 72-**74**, 75-76, 163
- privileged accounts and, 78, 81, 84
- risk-score approach and, 233
- role-based (RBAC), 9-11, 25-26, 62-**64**, 67, 81-83
- spectrum, **58**
- types, 62
- in utility industry, 219
- voice recognition for, 232

Access management, **4**, 11, 20, 27, 30, 44, 48, 57, 68, 231

Active Directory (AD), 8, 40, 105-106
- in access control, **26**-27, 197, 234
- authentication and, 42, 47, 62
- authorization and, 61
- data sharing and, 168, **170**, 182-**183**
- in IAM, **48**
- Microsoft Azure (Azure AD) and, 43, **92**, 97
- provisioning and, 21, 24

Actuators, 131-132, 137, 146-147, 149-150, 158-159, 164, 166, 219

Adaptive policy-based access management (APAM), 68-69, 74-75
- configuration, **69**

Amazon Web Services (AWS), 32, 92, 95-96, 99-101, 125, 191

Analytics and dashboards (in IAM), 12, **20**, 28

Android, **116**-118, 127

Approval workflow, 3, 17, 20, **23-24**, 38, 165, 173

Assurance level, 13, 31-32, 60-**61**, 80, 86, 111-112, 123-125, 139-140, 180, 189, 199, 229
- authentication and, **59**-60

Attestation reporting, 5, 11, **20**, 27
- governance, risk management, and compliance (GRC) and, **20**, 27-28

Attribute, 1-3, 9-11, 25, 60-62, 64-65, 70, 74, 226, 230-234
- and ABAC, 65-71, 83
- back-end (BAE), 200
- cloud and, 102-**104**, **106**
- in directories, 44-46, 52-55
- ICSs and, 162-163, 166

IoT and, 135, 139, 141
Authentication, 2, 4-5, 11-14, **20**, 32, 33, 36, 57-**58**, 67, 69, 127, 191-192, 235
in access control/management, 27-28, 62
Azure and, 97
biometrics and, 231-233
BYOD and, **117**, 120, 125, 127
cloud and, 29-30, 49-50, 90, 160, 198
consumerization and, 192, 194-195, 199, 229-230
directory, 8, 40, 42, 47-48
externalized, 44
federated, 6, 154, 223
FIDO and, 139-140, 233
IAM and, 6
information sharing and, 170, 174
levels of, 58-**59**, 60
OAuth and, 123-124
OpenID Connect for, 30-31, 122, 190
PAM systems and, 80
risk-based, 233
SAML and, **124**
three-legged, 31, 123-124
two-factor, 32-33, 89, 97, 98, 125-126, 139, 152, 160, 175, 230, 234
two-legged, 31, 123
Authentication-authorization spectrum, **58**
Authoritative data sources, 21
Authorization, 7, 11, 61-62, 83, 162, 198, 234
in access control/management, 27, **58**, 62, 65, 81-82
in approval workflow, 25, 35
BYOD and, 124
cloud and, 42
coarse-grained, 44, 61
fine-grained, 44, 47, 83, 162, 168
ICSs and, 162
OAuth and, 31
Azure, 32, 42-43, 89, **92**, 95-98, 125, 169
Azure AD, 42-43, 47, 52, **92**

B

Baby boomers, 14, 186-189, 223, 228
BlackBerry, **116**, 118
Bring your own device (BYOD), 109
access vs. security in, **113**
application management in, 115
device management in, 114-120, 128
device ownership continuum, **121**
information sharing and, 116
policy, 122, 129
pros and cons of, 120
strategy, 122, 161-162

C

Carnegie Mellon Capability Maturity Model (CMM), 33-35, **34**, 200-**201**
Certificate authority (CA), 169, **179**-181
Certificate revocation list (CRL), 179-180
Challenge-response, 25, 233
CIO—role in identity management, 12, 14-16
Cloud
-based identity service, 13, 29-30,

37, 41-42, 44, 51, 54-55, 87, 90, 97
benefits and dangers of, **159**
deployment, 101-104
hybrid, 41, 49-50, 91
identity management and, 1, 3, 12-13, 16, 29-30, 37, 40-44, 49-50, 51-54, 76, 85-87, 92-93, **104-106**, 160-161, 173-174, 199, 234
Internet of Things and, 135
migrating to, 29, 85
private, 91, 93, 158
protocols, 30, **104**
public, 60, 91, 190
service provider (CSP), 86, 90-91, 93, 95, 101, 105, 107, 135, 159-160
services, 29-30, 32, 40, 85-89, 91-93, 95, 102, 104-107, 159-160, 234
strategy, 93
Confidentiality-Integrity-Availability (CIA) model, 205-**206**
Consumer/citizen identity management (CIDM), 185
Consumerization, 1, 14, 185-204, 223, 227, 230
Consumers, 15, 110, 186, 190, 193, 202-203, 227-228, 230
Contractor, 5-6, 9-10, 36, 57, 81, 165-166, 190, 199
management, 5, 10, 36
provisioning, 9
Customer relationship management (CRM) and IdM, **186**
Cybersecurity, 35, 167, 205-208

D

Data loss, 37, 52, 57, 81, 122, 167, 171, 175, 183, 202, 209, 212
Data loss prevention (DLP), 81, 113, 167, **171**-172, 182-184, 206-208, 233-234
strategic approach to, 172
Data protection, 173-174
Data repository in IdM, 92, 231, 234
for cloud identity management, 34, 39, 45, 87, 89, 92, 103, 112, 173-174
secure, 168-**170**, 173-174, 182-183
Data sharing, **88**, 116, 167, 199, 218
benefits of a secure environment, 181
classification, 175
data-centric approach to, 173
information classification process, **176**
ISO 27001 and, 176-177
principles, 173
rights management and, **169**-171
security options for, 167-168
strategic approach for, 172
Data store, 13, 19, 26, 29-30, 35-37, 42, 46, 51, 55, 66-67, 80, 102, 106, 135, 137, 155, 163, 182, 194, 196, 216, 220, 229
Decision point, 7, 11, 44, 61-62, 67, 69-70, 76, 83
Device registration, 32, 125
Device types, 117-118
Digital transformation, 15, 35, 185, 204, 220
Directory
classic configuration, **48**-49
consumer, 51-52

design, 45-47
entries, 45
hybrid cloud configuration, **49**-50
models, 47-51
properties, 45
service, 6, 35, 39-44, 47-50, 52-54, 58, 97, 160
unified environment, 50-**51**

E

EC2, 99-100
Encryption, 13, 30, 49, 80, 115, 135, 140, 160-161, 169-**170**, 172, 174, 180, 225
Enterprise architecture, 10, 15, 53, 93-94, 102-103, 124, 127, 143, 161
cloud and, 53, 93-94, 102, 105, 161
Internet of Things and, 140, 143
Enterprise directory, 36, 40-43, 53
vs. authentication directory, 40
Enterprise mobility management (EMM), 119-120, 126, 129
Enterprise random password manager (ERPM), 78-79
Entitlement, 1, 7, 11, 17, **20**, 21, **24**, 25-28, 38, 47, 76, 82, 121, 172, 182, 199, **219**
management, 11, **20**, **70**-73
verification, 28
Entity management, 111-112
Entity relationship diagram, 10
Exfiltration, 113, 115-116, 171, 184, 207

F

Facebook, 13, 31, 55, 58, 123, 189, 191, 198
Fast IDentity Online (FIDO), 31-32, **104**, **116**, 124-125, **128**, 139-140, 190, 233-235
Federation, 6, 11-12, 30, **36**-37, 41, 45, 59, 81, 155, 232
industry-based, 29
Four-eyes policy, 76, 152, 180

G

Google identity management services, **92-93**
GoogleID, 13, 31, 55, 123, 189
Governance, 10-12, 15, 17, 36, 38, 45, 62, 65, 72, 83-84, 112, 124, 137, 164, 166, 224
Apple iOS and, 117
AWS CloudTrail and, 100
cloud and, 85, 87, 91, 94, 100-101, 105
information sharing and, 173, 175
IoT and, 136
mobile device management (MDM) and, 119
operational technology (OT) and, 155, 164, 166
risk, and compliance (GRC), **20**, 28
Sarbanes-Oxley Act (SOX) and, 209

H

Hardware security module (HSM), **179**-180
Health care, 43, 73, 83
consumerization and, 14, 197-198
privacy and, 213, 217-218, 221

I

IAM. *See* Identity and access management
IDentity as a Service (IDaaS), 29, 37, 50, 54, **90**, 93
  Okta, 54, **92-93**
  OneID, 54
  PingOne, 54, **92-93**
  Salesforce, 54, **92**, 191
Identity—what is, 1
Identity and access management (IAM), 2, **4**, 35, 81, 144, 182
  academia and, 198-199
  adaptive policy-based access management APAM and, **69**
  cloud and, 85-87, 89
  components, 5-7
  core features and capabilities, **19-28**
  defined, **4**
  directory infrastructure and, 53
  future of, 223
  health care and, 197
  IoT and, 30
  operational technology (OT) and, 149, 153
  strategy, 5
  XACML and, **70**
Identity attribute, 1-3, 7, 9-11, 20-21, 55, 83, 139, 187, 226, 230-232
  access control and, **62**, 64-71
  authentication and, 60, 62
  authorization and, 61-62
  back-end (BAE), 200
  cloud and, 29, 102-104, 106, 135
  consumer directory and, 52
  enterprise directory and, 40-41, 45-46, 53
  information sharing and, 172-173,
  OAuth and, 123
  operational technology (OT) and, 149, 157, 160, 162-**163**, 166
  policy and, 73-74
  roles and, 25
Identity data storage, 39, 192
  history of, 40
Identity management (IdM), 4, 6, 8, 11, 15-17, 20, 24, 27-29, 36-37, 94, 152, 231
  convergence with CRM, **186**
  defined, 2
  cloud and, 29-30, 160
  consumerization and, 188-191, 193, 198-199
  directory services and, 48
  environment, 3, 6, 15, 17, 37, 80-81, 105, 143, 178, 198-199, 231
  history, 40-41
  information sharing and, 168, 178
  IoT and, 143
  maturity level and, 33-35
  operational technology (OT) and, 152, 160
  privileged account management (PAM) and, 80-81
  workflow, 5, 8, 10-11, 17, 20, 23-26, 35
Identity proofing, 59-60
Identity provider service (IdP), 6, 11, 13-14, 29-31, 37, 108, 123, 154, 192-194, 199, 223, 229-230, 235
  authentication and, 70, 82, 89, 192
  cloud and, 50, 54-55, 87, 89-90, 92-94, 106, 160

IoT and, 139, 219
Industrial computer systems (ICS), 60, 135-136, 146, 149-166
inetOrgPerson, 45
Infrastructure as a service (IaaS), 90-91, 94, 107-108
Internet of Things (IoT), 1, 13, 30, 53, 131-147, 183, 228, 230
- actuators, 132
- architecture, 140
- best practices, 136
- big data analysis and, 135
- cloud and, 135, 160
- consumerization and, 190
- contributing technologies, 135
- effects of, 132-134
- industrial computer systems (ICSs) and, 149
- in home automation, 133
- infrastructure deployment, 144
- integrating with business processes, 144
- philosophy, 142
- questions to ask when assessing, 131
- regulation and, 219-220
- sensors, 132, 233
- strategy, 143

Intrusion detection system (IDS), 128, 146, 206-207
iOS, 116-118, 121, 127
IoT. *See* Internet of Things
IoT Security Foundation (IoTSF), 138

J

JSON, 43-44, 50, 53, 83, 104, 123-124

K

Kantara Initiative, 138-139
Key management, 13, 107, 163, 169, 179-180, 184
Know your customer (KYC), 14-15, 187-189, 195-196, 200-204, 220, 223
- continuum, **188**

L

LDAP, 12, 41, 43, 45, 47-51, 103, 137, 197
Least privilege (least rights) principle, 77-78, 173
Life management platform (LMP), 193, 196, 230
LinkedIn, 13, 31, 123, 191

M

Maturity assessment, 10, 33-37, 200-201
Microsoft Azure, 32, 42-43, 52, 89, 92, 95-98, 125, 169
Microsoft Live, 13, 55, 189, 198, 229
Millennials, 14, 109, 118, 186-189, 198, 201, 223, 228
Mobile device management (MDM), 113, 118-120, 122, 126, 128-129
Mobile devices, 3, 6, 12, 25, 190
- authentication, 44, 139, 232
- BYOD and, 109, 112-113, 115-117, 120-122, 125, 128-129, 161-162
- device ownership continuum, **121**
- information sharing and, 175
- protocols, 30-31, 123-124

management. See Mobile device management (MDM)
registration of, 32, 125
types, 117-118
Mobile strategy, 122-125

N

Network function virtualization (NFV), 14

O

OAuth, 6, 31, 42, 52, **104**, **116**, 123-**124**, 174-175, 190
vs. SAML, **124**
OData, 43-44, **51**, **104**, **106**
Onboarding, 5, 22
OpenID Connect, 6, 30-31, 53, **104**, **116**, 122-123, 174, 190
Operational technology (OT), 83, 146, 149-166, 219

P

Password management, 25, 78
Password vault, 78
Payment Card Industry (PCI), 52, **95**, 208
Personally identifiable information (PII), 8, 46, 52, **95**, 113, 214, 217-218, 221
privacy legislation principles and, **210-212**
Phablet, 109-110, 114, 126
PII. *See* Personally identifiable information
Platform as a service (PaaS), 90
Policy administration, 74-76, 82-83
manager, 47, 75
Policy components, **74**
Policy management, 7, 72, 75-76
in ABAC, 75
Privacy, 15, 110, 194, 202, 205, 209-219, 221, 228, 235
access control and, 65
data, 224-225, 228
definition of, 209
principles, **210-212**
industry regulation, 216-220, 226
legislation in different countries, 213-216
regulation, 3, 14, 29, 46, 55, 59, 65, **95**, 175, 197, 204, 206, **210**-213, 225
Privileged account management (PAM), 47, 76-79, 84, 160, 225
pros and cons, 79-80
strategic approach and, 80-81
Privileged identity management (PIM), 77-78
Privileges, 25, 47, 77-78, 80, 84, 90, 173
Protocols, 6, 42-45, 48, 50, 52-53, 68, 70, 83, 122-124, 137, 151, 179, 197-198
cloud, 30-32, 41, **92-93**, **104**,
Provisioning, 3-7, 12, 14, 17, 19, 28, 35-36, 55, 64, 81, 122, 220, 230
approval workflow and, 23-25
automation of, 23
cloud and, 29, 99, 106, 198
directory and, 46-47, 50
in an IAM environment, 20-23, 28
industrial computer systems (ICSs) and, 152, 154, 165
on-demand, 11
reasons for not developing, 8
role management and, 25
staff, 8

standards, 44-45
system capabilities (levels), 7-10
Public key infrastructure (PKI), 60, 169, 178-180, 184
environment, **179**
key management, 13, 107, 163, 169, 179-180, 184
registration for, 180
usage, 180

R

Registration authority (RA), 179-181
Regulation, 3, 14, 29, 46, 55, 59, 65, **95**, 175, 197, 204, 206, **210**-213, 225
Replication, 46-47
Reporting, 11, 21, 36, 42, 73-74, 119, **201**
attestation, 5, 11, **20**, 27-28
RESTful APIs, 44, 51, 99, 103-**104**
Rights management, 117, 168-170, 174, 176, 182-184, 208
vs. secure data, **170**
Risk management, 6, **20**, 28, 44, 60, 76, 162, 174, 181, 184
cloud and, 101, **106**
operational technology (OT) and, 162-163
Role management, 25-27
Role-based access control (RBAC), 10-11, 25, 63-65, 67, 83

S

SaaS. *See* Software as a service (SaaS)
SAML, 6, 29, 31, 41-42, 44, 47, 49-50, 52, **82**, 103-**104**, **106**, 123-**124**, 174, 198, 232
vs. OAuth, **124**
SCADA, 141, **150**, 161-162, 165
SCIM, 29, 44-45, 50, 52-53, 106, 198
Secure data repositories, 168
Secure data vs. rights management continuum, **170**
Security breach, 57, 84, 112, **157**, 181, 225
Security information and event management (SIEM), 81
Sensor, 132, 136-137, 142, **146**-147, 149, 158-159, 161, 163-164, 166, 190, 233
Single sign-on (SSO), 11, 30, 37, 48, 78, 80-81, 86, 95, 97, 106, 124
Smartphone, 12, 32-33, 160, 189-191, 202, 228, 232-233
access management and, 68
authentication and, **89**, 97
BYOD and, 109-118, **121**, 125-129, 161
cloud and, 100, **104**
compliance issues, 113
consumer strategy, 110
enterprise directory and, 53
enterprise strategy, 110
IoT and, 132-133, 139
security, 113
Social login, 6, 13, 31, 60, 123, 189, 191, 198, **203**
Social networking, 31, 123, 229
Software as a service (SaaS), 29, 41-42, 45, 49-50, 53-54, 89-90, **92**-94, **105-106**, **124**
Software-defined networking (SDN), 14, 108, 234
Synchronization, 13, 21, 29, 34,

41-43, 46-47, 52-53, 67, 87, 89, 97, **105-106**, 220
vs. replication, 46-47

T

Tablet, 104, 109, 113-114, **117**-118, 128, 161

U

Use case, 36, 54, 82, 105-106, 127-128, 146, 165, 182-183, 203, 220
for authentication, 58, 97
for directories, 40-43
for PKI, 180
User experience, 15, 37, **117**, 158, 186, 197-198, 201, 227

V

Virtual directory service (VDS), 35, 50, 55
Voice recognition, 33, 126, 232

W

Web access management (WAM), 20, 30, **48**
Windows, 40, 42, 48, 58, 88, 96-98, **105**, **116**, 118, 152, 168-169, 171, 181

X

XACML, 47, 68, **70**-72, 76, 83, 198
request structure, **70**
response structure, 71
XML, 50, 53, **71**, 74-75, 83, **104**, **124**, 137

Z

Zero-day start, 9, 21, 35