Index

Action plan, 109
  intermediate goals, 109
metrics, 110
Aligning security activities in Support of
  organizational objectives, 34, 134
Aligning security with business objectives, 11
Anchoring, 88
Annual loss expectancy (ALE), 43
Appropriateness, 153
Architecture, 49, 50
  for strategy development, 94
Asset classification, 39
Assurance process integration, 141
Audits, 93

Benchmarking, 44
Biased evaluation, 89
Board of directors, 70
  role of, 22
Business continuity planning/disaster
  recovery (BCP/DR), 39
Business focus, 50
Business impact assessment, 93, 140
Business process assurance/convergence,
  39, 47

Capability Maturity Model (CMM); see
  also CMM, 59
Level 4, 10
Chief Information Security Officer (CISO),
  24
general purpose, 25
  position responsibilities, 25
  reporting, 26
CISO decisions, 134
CMM, 82, 85
  for strategy development, 96
CobiT, 10, 58, 82
domains, 59
  acquire and implement, 59
  deliver and support, 59
  monitor and evaluate, 59
  plan and organize, 59
  for strategy development, 94
high-level control objectives, 60
  acquire and implement, 60
  deliver and support, 60
  monitor and evaluate, 60
  plan and organize, 60
levels, 60
  0—nonexistent, 61
  1—initial/ad hoc, 61
  2—repeatable but intuitive, 62
  3—defined process, 62
  4—managed and measurable, 62
  5—optimized, 63
Complexity, 49
Compliance, 124, 149
Compliance enforcement, 93
Compliance metrics, 146
Confirmation bias, 89
Control effectiveness and reliability, 140
Control failure, 154
Control reliability, 154
Controls, 44
Corporate Governance Task Force, 68
Criticality, 147
Cultural worldviews, 181
Cyber Security Task Force, 83
  responsibilities of the senior executive, 84
Efficiency, 153
Egalitarians, 181
Employees and users, 72
Endowment effect, 89
Event logging, 123
Executive management, 22
Executive team members, 70
Failed log-in enforcement, 121
False consensus, 89
Functionality, 153
Gap analysis, 84
Governance, 1, 9
  as management problem, 15
  benefits of, 11
  compliance, 18
  definition, 1, 5
  ensuring accountability for safeguarding critical assets, 13
  failures of, 17
  increasing predictability and reducing uncertainty of business operations, 15
  increasing the company’s worth, 14
  increasing trust of customers and stakeholders, 14
laws, 17
metrics, 27
objectives, 28
  ensuring that objectives are achieved, 29
origins of, 3
outcomes of, 6
providing assurance that critical decisions are not based on faulty information, 13
regulatory requirements, 18
responsibilities, 21
risks, 30
roles, 21
structure and framework, 12
verifying that resources are used responsibly, 31
why needed, 9
Group think, 89
Heirarchists, 181
Herding instinct, 89
implementation of IT strategy, 12
Inactivity timeout, 123
Inadequate performance, 110
Incident management and response metrics, 155
Incident management decision support metrics, 156
actions, 158
authority, 159
definition of incident, 156
disasters, 159
kind of incident, 157
most effective response, 158
multiple events and/or impacts, 158
notification, 159
response teams, 159
security incident, 157
severity level, 157
triage, 158
Independent information security program evaluation, 74
Individualists, 182
Information, 7
  value of, 7
Information security (IS), 2
  architectures, 50
  objectives of, 50
Information security governance, 5
Information security management metrics, 131
Information security management system (ISMS), 64
Information security operational metrics, 145
Information security outcomes, 33
defining outcomes, 33
Information security program development metrics, 127
Information security responsibilities, 23
### Index

**Information Technology Governance Institute (ITGI), 58**
Certified Information Security Manager Program, 58
ISO 17799 Code of Practice for Information Security, 67
ISO 27001, 64
ISO 27002, 67
ISO/IEC 27001, 63, 83
ISO/IEC 27002, 63, 83
IT and information security management, 145
IT Governance Institute, 11

- Key control effectiveness, 154
- Key goal indicator (KGI), 34
- absence of communication, 41
- contradictions, 41
- controls, 43
  - effectiveness, 43
  - number of, 44
  - utilization, 44
- cost of security, 43
- incidents, 41
- inconsistencies, 41
- number of management levels, 41
- security activities, 43
- security resources, 43

Layered security, 38
Layering, 50
Legal and regulatory requirements, 17
Log reviews, 45

- Management effectiveness, 154
- Management metrics, 132
- Mental accounting, 89
- Metrics, 27
  - ability to determine the effectiveness, efficiency, accuracy, and reliability of, 45
  - accuracy, 141
  - reliability, 153
- Modularization, 50

National Cyber Security Task Force, Information Security Governance, 68
Noncompliance, 123

**Number and frequency of subsequently discovered unreported incidents, 45**

Optimism, 88
Organizational risk tolerance, 139
Organizational unit reporting, 73
Organizational unit security program, 72
Overconfidence, 88

- Passwords, 120
  - backup and recovery, 122
  - change process, 121
  - control function, 121
  - expiration, 121
  - format, 120
  - generators, 122
  - resets, 122
  - reuse, 122
  - storage, 122
  - transport, 123
  - usage, 121
- Performance measurement, 45, 48
- Periodic risk assessment, 38
- Personnel competence, 152
- PINs, 120
- Policy development, 111

- Recovery time, 78
- Reengineering, 110
- Regulation, 18
- Regulatory compliance levels, 18
- Resource adequacy, 152
- Resource dependency analysis, 93
- Resource management, 44, 47, 144
- Resource utilization, 44
- Resource valuation, 139
- Risk assessment, 93
  - comprehensive, 140
- Risk exposure, 148
- Risk management, 36, 47, 137
  - current state, 84
    - executing appropriate measures, 137
    - managing risk appropriately, 76
    - metrics for, 138
    - objectives, 75, 77
    - responsibilities, 76
- Risks, 30
  - acceptable level, 36
  - business impact assessment, 38
Risks (continued)
defined risk appetite, 39
executing appropriate measures to
manage risk, 36
managing, 36
periodic risk assessment, 38
Road map, 50
ROSI, 42

SABSA, 82, 85
SABSA business attributes and metrics,
163
business strategy attributes, 177
legal and regulatory attributes, 173
management attributes, 165
operational attributes, 167
risk management attributes, 168
technical strategy attributes, 174
user attributes, 163
SABSA Matrix, 95
Security, 81
current state of, 81
Security architecture, 48
Security governance, 18, 47
objectives, 47
Security management decision support
metrics, 132
Security objectives, 45
Security program development metrics,
127
operational metrics, 129
Security steering committee, 24
Security strategy, 87
architecture, 92
attributes of, 89
audits., 93
awareness and education, 93
business impact assessment, 93
compliance enforcement, 93
controls, 92
countermeasures, 92
environmental security, 94
facilities, 94
failures, 88
guidelines, 92
layered defenses, 92
metrics and monitoring, 94
organizational structure, 92
organizational support and assurance
providers, 94
outsourced security providers, 94
personnel security, 92
policies, 92
procedures, 92
resource dependency analysis, 93
resources, 91
risk assessment, 93
roles and responsibilities, 93
skills, 93
standards, 92
technologies, 92
threat analysis, 93
training, 93
vulnerability analysis, 93
Selective recall, 89
Senior executive, 70
Senior managers, 71
Sensitivity, 147
Sherwood Applied Business Security
Architecture (SABSA); see also
SABSA, 51
attributes, 56
business security attributes, 57
development process, 54, 56
framework for security service
management, 54
life cycle, 54
matrix, 52
model, 51
Software Engineering Institute (SEI), 59
Standardized processes, 44
Standards, 116
attributes of, 116
classifications, 119
physical Access, 124
sample, 118
statement, 119
Status quo bias, 88
Strategic alignment, 34, 47, 134
Strategic direction, 28, 29
Strategic metrics, 27
Strategy constraints, 96
contextual, 97
operational, 97
Strategy development, 99
process, 100
Strategy implementation, 109
Strategy, elements of, 110
Tactical performance measures, 153
Threat analysis, 93
Threat and vulnerability management, 45
Time it takes to detect and report security-related incidents, 45
Unmitigated risk, 84
User communities, 120
Value delivery, 42, 47, 142
Vulnerability analysis, 93