
Index

A

- access, definition, 112
- action lists
 - presenting to senior managers, 233–234
 - refining, 234–235
 - reviewing, 232–233
- actors, definition, 112
- adaptable measures, 21–22
- analysis teams. *See also* champions; general staff; operational area managers; senior managers.
 - and computing infrastructure vulnerabilities, 36–37
 - floating, 272
 - interdisciplinary makeup, 32–33
 - makeup of, 12, 32–33, 65
 - purpose of, 13, 27
 - roles and responsibilities, 27–28, 65–66
 - selecting, 45, 64–65, 76–77
 - size, 65
 - skill sets, 27–28, 66–67
 - tailoring, 250, 272
 - training, 67–68
- analyzing risks. *See* conducting risk analysis.
- areas of concern
 - gap analysis, 131–134
 - grouping, 121–122
 - identifying, 93–96
 - mapping to critical assets, 128–131
- artifacts, tailoring, 250–254
- asset-based threat profiles, 13–14, 35–36
- asset-based threat trees, 112, 114–117
- asset-specific profiles, 112–113
- assets
 - definition, 112
 - identifying. *See* identifying assets; identifying key components; identifying organizational knowledge; workshops.
 - protecting. *See* conducting risk analysis.
- attributes of risk evaluation
 - analysis teams. *See also* champions; general staff; operational area managers; senior managers.
 - and computing infrastructure vulnerabilities, 36–37
 - floating, 272
 - interdisciplinary makeup, 32–33
 - makeup of, 12, 32–33, 65
 - purpose of, 13, 27

- attributes of risk evaluation (*cont.*)
 - roles and responsibilities, 27–28, 65–66
 - selecting, 45, 64–65, 76–77
 - size, 65
 - skill sets, 27–28, 66–67
 - tailoring, 250, 272
 - training, 67–68
 - business unit participation, 32–33
 - catalog of security practices
 - definition, 28
 - description, 84–86
 - examples, 443–455
 - tailoring, 250–251
 - catalog of vulnerabilities, 29, 159–160
 - collaboration, 33–34
 - defined evaluation activities, 29–30
 - definition, 18
 - documented evaluation results, 30
 - focus on risk, 31
 - focused activities, 31–32
 - generic threat profile, 28–29
 - information technology participation, 32–33
 - mapping to OCTAVE, 52–54
 - mapping to principles, 26
 - next steps, 30–31
 - organizational principles, 13–14, 32
 - scope of evaluations
 - description, 30
 - focus on the critical few, 23
 - setting, description, 45
 - setting, role of analysis teams, 65–66
 - setting, selecting operational areas, 68–69, 77–78
 - senior management participation, 33
 - summary table of, 19, 53–54
 - technological principles, 32
 - auditing security. *See* conducting risk analysis.
- B**
- brainstorming asset identification, 89–92
 - briefing participants, 73
 - business unit participation, 32–33
- C**
- case studies and scenarios
 - Company S, 257–265
 - Company SP, 267–270
 - Company X, 265–267
 - disgruntled employee, 4–5
 - MedSite scenario, 56–58, 311–361
 - network sabotage, 4–5
 - professional societies, 270–272
 - risk profile examples
 - expected values, 223
 - mitigation plan, 211–212, 215
 - multiple impacts, 249
 - technological vulnerabilities, 253
 - sample schedules, 74–75
 - worksheet examples, 363–442
 - catalog of
 - security practices
 - definition, 28
 - description, 84–86
 - examples, 443–455
 - tailoring, 250–251
 - vulnerabilities, 29, 159–160
 - categorizing assets, 88–89
 - champions, 60–61
 - collaboration, 33–34
 - collaborator access, 273
 - Common Vulnerability and Exposure (CVE), 160
 - communication, openness. *See* open communication.
 - Company S scenario, 257–265
 - Company SP scenario, 267–270
 - Company X scenario, 265–267
 - components, identifying for evaluation. *See* evaluating selected components; identifying key components.
 - computing infrastructure, vulnerability. *See* vulnerability.
 - conducting risk analysis. *See also* OCTAVE.
 - activities, 9–10, 50, 171
 - analysis aspect, 13–14
 - aspects of, 6–7, 13–14
 - assets, identifying. *See* identifying assets.
 - attributes. *See* attributes of risk evaluation.
 - components, selecting. *See* evaluating selected components; identifying key components.
 - computing infrastructure vulnerability. *See* vulnerability.
 - current status, identifying. *See* identifying organizational knowledge; workshops.
 - definition, 9

- flowchart, 50
 - of information. *See* information security.
 - limited evaluations, 64
 - organizational principles, 11–12, 13–14
 - outputs. *See* outputs.
 - overview, 170
 - participants. *See* personnel requirements.
 - phase descriptions, 13–14
 - principles. *See* principles, risk evaluation.
 - process descriptions, 46–51
 - results. *See* developing protection strategies; results.
 - return on investment, 64
 - risk evaluation criteria, 175–179
 - risk management. *See* risk management.
 - role in information security, 10–11
 - scheduling, 74–76
 - scope. *See* scope of evaluations.
 - selecting components. *See* evaluating selected components; identifying key components.
 - statistics. *See* probability.
 - technological aspect, 11–12, 14
 - threat impacts. *See* impacts.
 - threats, identifying. *See* threat profiles; threats.
 - workshops, 170–171
 - configuration vulnerability, 139–141
 - consolidating
 - asset information, 111, 118–122, 194–197
 - multiple evaluation results, 272
 - strategy information, 197–199
 - continuous processes, 22
 - costs of security breaches, 3
 - creating threat profiles
 - access, definition, 112
 - activities, 48, 111
 - actors, definition, 112
 - asset-based threat trees, 112, 114–117
 - asset-specific profiles, 112–113
 - assets, definition, 112
 - consistency and completeness, 135
 - consolidating asset information, 111, 118–122
 - generic threat profile, 112
 - hardware assets, 136
 - information assets, 135
 - motives, definition, 112
 - outcomes, definition, 112
 - overview, 110
 - people assets, 136
 - profile properties, 112
 - software assets, 136
 - systems assets, 136
 - threat sources, 113
 - workshops, 110–112
 - critical assets. *See also* identifying assets.
 - consistency across, 136
 - describing, 125
 - gap analysis, 131–134
 - identifying, 122–123
 - identifying threats to, 128–134
 - prioritizing, 126–128
 - protecting. *See* conducting risk analysis.
 - security requirements, 125–128
 - selecting, 122–124
 - threat impacts, 172–175
 - threat probability, 187–190
 - threat profiles, 135–136
 - cultural principles, 20, 24–25
 - current status, identifying. *See* conducting risk analysis; identifying assets; identifying organizational knowledge; workshops.
 - customer access, 273
 - customizing OCTAVE. *See* OCTAVE, tailoring.
 - CVE (Common Vulnerabilities and Exposures), 160
- D**
- defined processes, 22
 - design vulnerability, 139–141
 - developing protection strategies. *See also* conducting risk analysis.
 - action lists
 - creating, 217–220
 - presenting to senior managers, 233–234
 - refining, 234–235
 - reviewing, 232–233
 - activities, 51, 193, 229
 - assigning responsibility, 218
 - compiling survey results, 194–197
 - consolidating asset information, 194–197
 - consolidating strategy information, 197–199
 - description, 201–202
 - incorporating strategic themes, 216–217

developing protection strategies (*cont.*)

- next steps, creating, 235–237
 - for operational practice areas, 205–208
 - order of processes, 220
 - outputs of risk evaluation, 37–39
 - overview, 192, 228
 - phase description, 14, 37–39
 - presenting to senior managers, 230–234
 - refining, 234–235
 - reviewing risk information, 199–200
 - reviewing strategy plans, 232–233
 - risk management, 283–284
 - risk management approach, 8
 - risk mitigation plans
 - description, 208–209
 - ensuring consistency, 214–215
 - expected loss values, 221–222
 - impact values, 209
 - numerical values for qualitative data, 224–225
 - presenting to senior managers, 233–234
 - prioritizing losses, 221
 - probability, 220–226
 - refining, 234–235
 - relative rankings, 224–225
 - reviewing, 232–233
 - selecting actions, 213–214
 - selecting an approach, 209–212
 - in small organizations, 263
 - tending toward medium, 222–224
 - uncertainty, 225
 - in small organizations, 263
 - for strategic practice areas, 203–205
 - workshops, 192–193, 228–229, 236–237
- disgruntled employee scenario, 4–5
- due care standards, 63–64

E

- evaluating selected components. *See also*
 - conducting risk analysis; identifying key components.
- activities, 49, 158–159
- overview, 158
- tailoring evaluations, 245–250
- workshops, 158–159

evaluation teams. *See* analysis teams.

examples. *See* case studies and scenarios.

expected loss values, 221–222

external security breeches, 3–4

F

- floating analysis teams, 272
- focus on risk, 31
- focus on the critical few, 23, 109. *See also* scope of evaluations.
- focused activities, 31–32
- follow-up activities. *See* developing protection strategies.
- forward-looking view, 23
- frequency of security breeches, 3

G

- gap analysis
 - threats to critical assets, 131–134
 - vulnerability evaluation results, 166–168
- general staff. *See also* analysis teams; operational area managers; senior managers.
 - knowledge elicitation workshops, 47
 - selecting, 72–73, 77–78
- generic threat profile. *See also* threat profile.
 - creating, 112
 - description, 28–29
 - tailoring, 251–252
- global perspective, 25
- Gramm-Leach-Bliley legislation, 63
- grouping
 - assets, 118–119
 - security requirements, 119–121

H

- hardware assets. *See also* identifying assets.
 - definition, 88
 - protecting. *See* conducting risk analysis.
 - security requirements, 102
 - threat profile for, 136
- HIPAA (Health Information Portability and Accountability Act), 63
- hiring outside evaluators. *See* outsourcing.

I

- identifying assets. *See also* identifying organizational knowledge; workshops.

- brainstorming, 89–92
- categorizing assets, 88–89
- compiling a list, 89–92
- critical assets
 - consistency across, 136
 - describing, 125
 - gap analysis, 131–134
 - identifying, 122–123
 - identifying threats to, 128–134
 - prioritizing, 126–128
 - security requirements, 125–128
 - selecting, 122–124
 - threat impacts, 172–175
 - threat probability, 187–190
 - threat profile for, 135–136
- definition, 87
- grouping
 - assets, 118–119
 - security requirements, 119–121
- hardware assets
 - definition, 88
 - security requirements, 102
 - threat profile for, 136
- information assets
 - definition, 87
 - security requirements, 101
 - threat profile for, 135
- people assets
 - definition, 88
 - security requirements, 102–103
 - threat profile for, 136
- prioritizing assets, 92–93
- security requirements
 - grouping, 119–121
 - hardware assets, 102
 - identifying, 97–99
 - information assets, 101
 - people assets, 102–103
 - prioritizing, 99–100
 - software assets, 102
 - systems assets, 101
- software assets
 - definition, 87
 - security requirements, 102
 - threat profile for, 136
- systems assets
 - definition, 87
 - security requirements, 101
 - threat profile for, 136
- identifying key components. *See also* conducting risk analysis; evaluating selected components.
 - activities, 48–49, 139
 - component classes, 142–150
 - overview, 138
 - systems of interest
 - identifying, 143–144
 - multiple, 144–146
 - technology vulnerabilities. *See* vulnerability workshops, 138–139
- identifying organizational knowledge. *See also* identifying assets; workshops.
 - activities, 83–84
 - areas of concern
 - gap analysis, 131–134
 - grouping, 121–122
 - identifying, 93–96
 - mapping to critical assets, 128–131
 - catalogs of security practices, 28, 84–86
 - current security practices, 103–107
 - flowchart, 47
 - general staff, 47
 - impact assessment, 96–97
 - operational area managers, 46
 - organizational vulnerabilities, 103–107
 - overview, 82
 - senior managers, 46
- impacts
 - assessing, 96–97
 - on critical assets, 172–175
 - definition, 171
 - multiple values, tailoring, 248–249
 - relative values, 209
 - threat outcomes, 171–172
- implementation vulnerability, 139–141
- information assets. *See also* identifying assets.
 - definition, 87
 - protecting. *See* conducting risk analysis.
 - security requirements, 101
 - threat profile for, 135
- information security. *See also* conducting risk analysis.
 - breeches, 3–4
 - definition, 5

information security (*cont.*)
 principles. *See* principles, risk evaluation.
 and probability, 185–187
 regulations, 63–64
 return on investment, 64
 standards of due care, 63–64
 third party support for. *See* outsourcing.
 information systems audits, 6
 information technology participation, 32–33
 integrated management, 23–24
 integrated Web portal service providers, tailoring
 OCTAVE, 267–269
 internal security breeches, 3–4

K

knowledge elicitation workshops,
 46–48

L

law of large numbers, 184

M

managed service providers, 7–8
 management involvement. *See* operational area
 managers; senior managers.
 mapping
 areas of concern to critical assets,
 128–131
 attributes to OCTAVE method,
 52–54
 attributes to principles, 26
 computing infrastructure, 141–142
 network topology, 141–142
 outputs to OCTAVE method, 54–56
 principles to attributes, 26
 MedSite scenario, 56–58, 311–361
 middle management involvement. *See* operational
 area managers.
 mitigation plans. *See* risk mitigation plans.
 monitoring risks, 285–286
 motives, definition, 112
 multiple impact values
 risk profile, example, 249
 tailoring, 248–249

N

network sabotage scenario, 4–5
 network topology, 141–142

next steps, creating, 235–237. *See also* developing
 protection strategies.
 numerical values for qualitative data, 224–225

O

OCTAVE. *See also* workshops; *entries for specific
 activities.*

attributes. *See* attributes of risk evaluation.
 common elements, 14–16
 history of, xxvi–xxviii
 mapping attributes to, 52–54
 mapping outputs to, 54–56
 nonlinear nature, 51–52
 outputs. *See* outputs.
 overview, 44–45
 participants. *See* personnel requirements.
 phase descriptions, 46–52
 preparing for, 45–46, 60–61
 principles. *See* principles, risk evaluation.
 and probability, 187–190
 processes. *See* processes.
 self-direction, 12
 tailoring
 analysis teams, 250, 272
 artifacts, 250–254
 automated tools, 250
 catalog of practices, 250–251
 evaluations, 245–250
 generic threat profile, 251–252
 for integrated Web portal service providers,
 267–269
 for large organizations, 265–267, 270–272
 multiple impact values, 248–249
 outsourcing, 248
 overview, 242–244
 physical security vulnerabilities,
 247
 policy reviews, 246
 processes, number of, 261–263
 processes, order of, 245–246
 range of possibilities, 242
 risk probability, 248
 schedules, 246–247
 for small organizations, 257–265, 270–272
 worksheets, 252
 workshops, 247
 variations on, 14

OCTAVE Method Implementation Guide, 67

- open communication
 - importance of, 24–25
 - risk management, 71, 277–279
 - operational area managers. *See also* senior managers.
 - knowledge elicitation workshops, 46
 - selecting, 72, 77–78
 - Operationally Critical Threat, Asset, and Vulnerability Evaluation. *See* OCTAVE.
 - organizational knowledge, identifying. *See* identifying organizational knowledge.
 - organizational principles. *See* principles, organizational.
 - organizations
 - large
 - managing common systems, 273
 - tailoring OCTAVE, 265–267, 270–272
 - sharing facilities, 273–274
 - small
 - computing infrastructure vulnerability, 262
 - critical assets, sample risk profile, 264
 - developing protection strategies, 263
 - developing risk mitigation plans, 263
 - tailoring OCTAVE, 257–265, 270–272
 - outcomes, definition, 112
 - outputs
 - asset-based threat profiles, 35–36
 - computing infrastructure vulnerabilities, 36–37
 - definition, 18
 - mapping to OCTAVE method, 54–56
 - phases of, 34–39
 - strategies and plans, 37–39
 - summary table of, 19, 55
 - outsourcing evaluations, 7–8, 248, 260–261
- P**
- participants. *See* personnel requirements.
 - people assets. *See also* identifying assets.
 - definition, 88
 - protecting. *See* conducting risk analysis.
 - security requirements, 102–103
 - threat profile for, 136
 - personnel requirements. *See also* analysis teams; champions; general staff; operational area managers; senior managers.
 - briefing participants, 73
 - selecting participants, 69–73
 - summary table of, 70
 - for workshops, 45–46, 70–71
 - phase 1. *See* asset-based threat profiles.
 - phase 2. *See* vulnerability, computing infrastructure.
 - phase 3. *See* developing protection strategies.
 - phase descriptions, 46–52
 - plans. *See* developing protection strategies.
 - policy reviews, tailoring, 246
 - principles
 - organizational
 - definition, 20
 - description, 24–25
 - risk evaluation attributes. *See* attributes of risk evaluation.
 - risk evaluation
 - adaptable measures, 21–22
 - continuous processes, 22
 - cultural principles, 20, 24–25
 - defined processes, 22
 - definition, 18
 - focus on the critical few, 23
 - forward-looking view, 23
 - global perspective, 18, 21–22
 - information security, 18, 21–22
 - integrated management, 23–24
 - mapping to attributes, 26
 - open communication, 24–25, 71
 - organizational principles, 20, 24–25
 - risk management, 20, 22–24
 - self-direction, 21
 - summary table, 19
 - teamwork, 25
 - risk management
 - definition, 20
 - focus on the critical few, 23
 - forward-looking view, 23
 - integrated management, 23–24, 277–279
 - open communication, 277–279
 - technological, 32
 - prioritizing
 - assets, 92–93, 126–128
 - loses, 221

- probability
 - classical concept, 184
 - and critical assets, 187–190
 - definition, 184
 - expected loss values, 221–222
 - frequency interpretation, 184–185
 - and information security, 185–187
 - law of large numbers, 184
 - numerical values for qualitative data, 224–225
 - and OCTAVE, 187–190
 - precautions for using, 225–226
 - qualitative analysis, 224–225
 - quantitative analysis, 221–222, 225
 - relative rankings, 224–225
 - risk, tailoring, 248
 - in risk mitigation plans, 220–226
 - subjective, 185
 - tending toward medium, 222–224
 - uncertainty, 225
 - process 1. *See* identifying organizational knowledge.
 - process 2. *See* identifying organizational knowledge.
 - process 3. *See* identifying organizational knowledge.
 - process 4. *See* creating threat profiles.
 - process 5. *See* identifying key components.
 - process 6. *See* evaluating selected components.
 - process 7. *See* conducting risk analysis.
 - process 8. *See* developing protection strategies.
 - processes
 - descriptions, 46–51
 - number of, tailoring, 261–263
 - order of, tailoring, 245–246
 - professional societies, 270–272
 - profile properties, 112
 - profiles. *See* risk profile; threat profile; generic threat profile.
 - protection strategies. *See* developing protection strategies.
- R**
- regulations for information security, 63–64
 - reporting results. *See* results.
 - responsibility for information security. *See also* analysis teams; champions; general staff; operational area managers; senior managers.
 - developing protection strategies, 218
 - risk management, 280–281
 - results
 - attributes of risk evaluation, 30
 - multiple evaluations, consolidating, 272
 - presenting to senior managers
 - action lists, 233–234
 - protection strategies, 230–234
 - risk mitigation plans, 233–234
 - surveys
 - compiling, 194–197
 - input to protection strategies, 194–197
 - interpreting, 196–197
 - vulnerability evaluation
 - actions and recommendations, 166–167
 - gap analysis, 166–168
 - reporting, 163–165
 - reviewing, 165–168
 - return on investment, 64
 - risk. *See also* information security; OCTAVE.
 - to assets. *See* assets.
 - components of, 13
 - definition, 8, 171
 - evaluating. *See* conducting risk analysis.
 - impacts of. *See* impacts.
 - threat sources. *See* threats.
 - vulnerability to. *See* vulnerability.
 - risk evaluation attributes. *See* attributes of risk evaluation.
 - risk evaluation criteria, 175–179
 - risk evaluation principles. *See* principles, risk evaluation.
 - risk management
 - after OCTAVE analysis, 279
 - analyzing risks. *See* conducting risk analysis.
 - assigning responsibility, 280–281
 - controlling risks, 286–288
 - definition, 8
 - identifying risks, 281–282
 - implementing, 8, 284–285
 - integrated management, 277–279
 - introduction, 276
 - monitoring, 285–286
 - open communication, 277–279
 - planning. *See* developing protection strategies.
 - principles of

- definition, 20
- focus on the critical few, 23
- forward-looking view, 23
- integrated management, 23–24, 277–279
- open communication, 277–279
- role in information security, 10–11
- time between evaluations, 288–290
- risk mitigation plans
 - description, 208–209
 - ensuring consistency, 214–215
 - expected loss values, 221–222
 - impact values, 209
 - numerical values for qualitative data, 224–225
 - presenting to senior managers, 233–234
 - prioritizing losses, 221
 - probability, 220–226
 - refining, 234–235
 - relative rankings, 224–225
 - reviewing, 232–233
 - selecting actions, 213–214
 - selecting an approach, 209–212
 - tending toward medium, 222–224
 - uncertainty, 225
- risk profile
 - definition, 182
 - examples
 - critical assets, small organizations, 264
 - expected values, 223
 - mitigation plan, 211–212, 215
 - technological vulnerabilities, 253
- roles for information security. *See* analysis teams; champions; general staff; operational area managers; senior managers.

S

- sabotage scenario, 4–5
- samples. *See* case studies and scenarios.
- scenarios. *See* case studies and scenarios.
- schedules
 - MedSite scenario, 78–79
 - risk analysis, 74–76
 - tailoring, 246–247
 - time between evaluations, 288–290
 - workshops, 75–76
- scope of evaluations
 - description, 30
 - focus on the critical few, 23
- setting
 - description, 45
 - role of analysis teams, 65–66
 - selecting operational areas, 68–69, 77–78
- security
 - evaluating. *See* conducting risk analysis.
 - of information. *See* information security.
- security practices
 - catalog of
 - definition, 28
 - description, 84–86
 - examples, 443–455
 - tailoring, 250–251
 - definition, 84
 - identifying current. *See* conducting risk analysis; identifying organizational knowledge; workshops.
 - operational, 85
 - strategic, 85
 - surveys
 - compiling results, 194–197
 - input to strategy development, 202–203
 - interpreting results, 196–197
 - security policy survey, 103–104
- security requirements
 - critical assets, 125–128
 - definition, 98
 - grouping, 119–121
 - hardware assets, 102
 - identifying, 97–99
 - information assets, 101
 - people assets, 102–103
 - prioritizing, 99–100
 - software assets, 102
 - systems assets, 101
- self-direction, 12, 21
- senior managers. *See also* operational area managers.
 - creating next steps, 235–237
 - importance to success, 33, 45
 - knowledge elicitation workshops, 46
 - obtaining sponsorship, 61–63
 - presenting action lists, 233–234
 - presenting protection strategies, 230–232
 - roles in evaluation, 33
 - selecting, 71, 77–78
- software assets. *See also* identifying assets.
 - definition, 87

software assets (*cont.*)
 protecting. *See* conducting risk analysis.
 security requirements, 102
 threat profile for, 136
 sources of security breaches, 3
 sponsorship from senior managers, 61–63
 staff requirements. *See* analysis teams; champions;
 general staff; operational area managers;
 senior managers.
 standards of due care, 63–64
 statistics. *See* probability.
 strategies. *See* developing protection strategies.
 success factors
 asset identification, 87
 knowledge elicitation workshops, 45–46
 scope of evaluations, 45
 senior management participation, 33, 45
 summary list of, 60
 surveys
 compiling results, 194–197
 input to strategy development, 202–203
 interpreting results, 196–197
 security policy survey, 103–104
 systems assets. *See also* identifying assets.
 definition, 87
 protecting. *See* conducting risk analysis.
 security requirements, 101
 threat profile for, 136
 systems of interest. *See also* evaluating
 selected components; identifying key
 components.
 identifying, 143–144
 multiple, 144–146

T

tailoring OCTAVE. *See* OCTAVE, tailoring.
 teams. *See* analysis teams.
 teamwork, 25
 technological principles, 32
 third party support for evaluations.
 See outsourcing.
 threat profile. *See also* risk profile.
 asset-based, 13–14, 35–36
 creating. *See* creating threat profiles.
 critical assets, 135–136
 generic
 creating, 112
 description, 28–29

 tailoring, 251–252
 hardware assets, 136
 information assets, 135
 people assets, 136
 software assets, 136
 systems assets, 136
 threats
 to critical assets, identifying,
 128–134
 definition, 93
 evaluating. *See* conducting risk analysis.
 impacts of, 171–172
 outcomes of, 94–95
 sources of, 94–95, 113
 timing. *See* schedules.
 tools for evaluating vulnerability
 list of, 154–156
 running, 161–162
 tailoring, 250
 training analysis teams, 67–68

V

vulnerability, computing infrastructure. *See also*
 conducting risk analysis.
 analysis team duties, 36–37
 assessing, 6
 catalogs of, 29, 159–160
 configuration vulnerability, 139–141
 customer/collaborator access, 273
 CVE (Common Vulnerabilities and Exposures),
 160
 design vulnerability, 139–141
 evaluating selected components, 49
 evaluation results
 actions and recommendations, 166–167
 gap analysis, 166–168
 reporting, 163–165
 reviewing, 165–168
 identifying, 48, 103–107
 implementation vulnerability, 139–141
 network topology, 141–142
 phase description, 14, 36–37
 physical security, 247
 selecting evaluation approach, 153–154
 selecting key components, 48, 150–153
 in small organizations, 262
 tools for evaluating
 list of, 154–156

running, 161–162

tailoring, 250

W

Web portal service providers, tailoring OCTAVE,
267–269

worksheets

examples, 363–442

tailoring, 252

workshops. *See also* identifying assets; identifying
key components; identifying
organizational knowledge.

conducting risk analysis,

170–171

creating threat profiles, 110–112

developing strategies, 192–193, 228–229,
236–237

evaluating selected components, 158–159

flowchart, 44

identifying key components,
138–139

knowledge elicitation, 46–48

overview, 44–45

personnel requirements, 45–46,
70–71

scheduling, 75–76

selecting participants, 45–46,
70–71

size, 72–73

tailoring, 247