

- Public Key Cryptography
  - Standards (PKCS), 626
  - public key infrastructure (PKI)
    - certificate authorities, 360–362
    - code repositories, 1144
    - digital certificates, 359–360
    - key management, 364–367
    - overview, 359
    - registration authorities, 362
    - steps, 362–364
  - public keys
    - asymmetric key cryptography, 335
    - hybrid methods, 347–348
    - RSA, 340–341
  - public relations factor in incident response teams, 1001
  - public switched telephone networks (PSTNs), 582–583, 682–683
  - Purpose Specification Principle in OECD, 142
  - PVC (polyvinyl chloride) jacket covering, 653
  - PVCs (permanent virtual circuits), 549
  - Python programming language, 1121–1122

## Q

- QA (quality assurance) in software development, 1080
- QKD (quantum key distribution), 344
- QoS (Quality of Service)
  - ATM, 551–552
  - availability, 1050–1051
- qualitative risk analysis
  - description, 72
  - overview, 76–78
  - quality, defined, 1117
  - quality assurance (QA) in software development, 1080
- Quality of Service (QoS)
  - ATM, 551–552
  - availability, 1050–1051
- quantifiability of security metrics, 854
- quantifying security, 851–853
- quantitative risk analysis
  - description, 72
  - vs. qualitative, 78–79
  - results, 75–76
  - steps, 73–75
- quantitatively managed level in CMMI, 1108
- quantum cryptography, 344–346
- quantum key distribution (QKD), 344
- queries
  - DNS, 527–528, 616
  - URLs, 615
- quorum authentication

description, 34  
PKI, 366–367

## R

RA (Requesting Authority) in SPML, 778  
race conditions  
description, 821  
processes, 717  
RAD (Rapid Application Development)  
methodology, 1099–1100  
radio frequency interference (RFI)  
electric power, 450  
twisted-pair cabling, 649–650  
RADIUS (Remote Authentication Dial-In  
User Service)  
network devices, 501  
overview, 789–790  
vs. TACACS, 791–793  
rainbow tables for passwords, 721–722  
raking locks, 922–923  
ramifications with compliance, 158–161  
random access memory (RAM) for Trusted  
Platform Modules, 405  
random numbers in cryptology, 327  
random password generation, 736  
random values in quantum cryptography, 345  
ransomware  
cryptography, 375  
protecting backups from, 897–898  
TLS, 604  
Rapid Application Development (RAD)  
methodology, 1099–1100  
rapid prototyping in software  
development, 1096

## ▲Index

1301

RARP (Reverse Address Resolution  
Protocol), 519  
RAs (registration authorities), 360, 362  
RB-RBAC (rule-based access control), 774  
RBAC (role-based access control) model, 771  
characteristics, 776  
core, 772  
hierarchical, 772–773  
RDP (Remote Desktop Protocol)  
overview, 700  
threat intelligence, 943  
RDS (Remote Desktop Services), 943  
reactive searching in threat hunting, 943  
real power, 671  
Real-time Transport Protocol (RTP), 689, 691  
real user monitoring (RUM) vs. synthetic

- transactions, 832
- realms in Kerberos, 785
- rebar, 439
- reciprocal agreements in disasters recovery, 1047–1048
- recommendations in reports, 873
- reconnaissance stage in Cyber Kill Chain model, 387, 994
- recording forensics investigation interviews, 1019
- recover function in Framework Core, 182
- recovery
  - data loss prevention, 269
  - incidents, 998
  - risk responses, 85, 87
  - recovery point objective (RPO)
    - disaster recovery, 1031–1032
    - high availability, 1052
  - recovery strategies
    - availability, 1049–1053
    - business process recovery, 1033–1034
    - data backups, 1034–1041
    - documentation, 1041–1042
    - overview, 1029–1033
    - vs. preventive measures, 1033
  - reciprocal agreements, 1047–1048
  - recovery site strategies, 1043–1047
  - redundant sites, 1048–1049
  - recovery teams in disaster recovery plans, 1056
  - recovery time objective (RTO)
    - disaster recovery, 1031–1033
    - high availability, 1052
- rectilinear filters in QKD, 344
- recursive queries in DNS, 527, 616
- red teaming
  - exercises, 902
  - penetration tests, 827–828
- redirect servers in SIP, 691
- reduced-function devices (RFDs), 570
- reduction analysis in threat modeling, 386–387
- redundancy for quality of service, 1050–1051
- redundant lighting, 912
- redundant sites, 1048–1049
- REEs (rich execution environments), 408–409
- reference monitors, 766
- references for candidates, 37
- reflection attacks in DNS, 620
- registered ports, 507
- registered trademarks, 150
- registrar servers in SIP, 689–690
- registration authorities (RAs), 360, 362
- registration of accounts, 738–740

- regression analysis in artificial intelligence tools, 977
- regression testing in software development, 1091
- regulations. See laws and regulations
- regulatory investigation requirements, 162
- regulatory policies, 30
- reinforcing bar, 439
- relevance
  - evidence admissibility, 1013
  - security metrics, 854
- relevant characteristic in threat intelligence, 941
- reliability
  - disaster recovery, 1051-1052
  - evidence admissibility, 1013-1014
  - TCP vs. UDP, 506
- religious law system, 128
- relocation teams in disaster recovery plans, 1056
- relocking function for safes, 222
- remanence, data, 240-244
- remediate phase in software vulnerability scans, 901
- remediation
  - incidents, 999
  - vulnerabilities, 871

#### ▲CISSP All-in-One Exam Guide

- 1302
- remote access
  - desktop virtualization, 699-701
  - Diameter, 793-795
  - overview, 696, 789
  - RADIUS, 789-790
  - TACACS, 790-793
  - VPNs, 697-699
  - Remote Authentication Dial-In User Service (RADIUS)
    - network devices, 501
    - overview, 789-790
    - vs. TACACS, 791-793
  - Remote Desktop Protocol (RDP)
    - overview, 700
  - threat intelligence, 943
  - Remote Desktop Services (RDS), 943
  - remote desktops, 700
  - remote journaling for backups, 1039
  - remote logging, 831
  - remote procedure calls (RPCs), 703-704
  - remote terminal units (RTUs)
    - DNP3, 626
  - industrial controls, 290

- SCADA systems, 294
- removal tools in forensics field kits, 1015
- repeaters
  - characteristics, 665
  - description, 655–656
- replay attacks
  - cryptography, 372–374
  - description, 787
- replication
  - backups, 1039–1040
  - logs, 831
- reports
  - digital forensics, 1021–1022
  - executive summaries, 872–875
  - incident response, 993
  - incidents, 997–998
  - overview, 869–870
  - penetration testing, 825
  - risk, 94–95
  - security results, 870–872
  - technical, 872–873
- repositories
  - backups, 1039
  - code, 1143–1144
  - identity, 739

- Representational State Transfer (REST), 615–616
- repudiation category in STRIDE model, 388
- reputation-based protection for antimalware software, 971
- reputation factor
  - disaster recovery, 1054
- outsourced security services, 974
- request methods in HTTP, 614
- Requesting Authority (RA) in SPML, 778
- requests in change management, 891
- requirements gathering in SDLC, 1080, 1082–1083
- resets for passwords, 737–738
- residual risk vs. total risk, 81
- resilience
  - data loss prevention, 272
  - system, 1051
- resolvers in DNS, 527–528
- resource owners in OAuth, 782
- resource protection
  - backups, 896–899
  - overview, 895–896
  - source files, 896
  - system images, 896
- resource records in DNS, 525
- resource servers in OAuth, 782
- respond function in Framework Core, 182

- responses
  - disaster recovery plans, 1055
  - incidents, 996
  - physical security, 908
  - risk. See risk responses
  - site planning, 424
  - SOAR, 980
  - responsibility
    - description, 161
    - disaster recovery goals, 1053
    - organizational. See organizational roles and responsibilities
    - responsive area illumination, 912
  - REST (Representational State Transfer), 615–616
  - restoration
    - backups, 1037, 1041–1042
    - disaster recovery plans, 1058–1060
    - restoration teams in disaster recovery plans, 1056

## ▲Index

- 1303
- restricted areas, 443
- results, analyzing, 870–872
- retention
  - assets, 228–230
  - data, 233–236
- retina scans, 727
- reusability in object-oriented programming, 1127
- reuse methodology in software development, 1105
- Reverse Address Resolution Protocol (RARP), 519
- reverse engineering attacks
  - in cryptography, 371
- reverse engineering patches, 905
- reverse proxies, 664
- reviews
  - audits, 743–744
  - change management, 892
- RFDs (reduced-function devices), 570
- RFI (radio frequency interference)
  - electric power, 450
  - twisted-pair cabling, 649–650
- rich execution environments (REEs), 408–409
- right to be forgotten provision in GDPR, 144
- right to be informed provision in GDPR, 144
- right to restrict processing provision in GDPR, 144
- ring topology, 489
- RIP (Routing Information Protocol), 535

- risk
  - defined, 9
  - FAIR, 179
  - frameworks, 172-179
  - ISO/IEC 27005, 177-179
  - metrics, 854
  - OCTAVE, 178-179
  - Spiral methodology, 1098-1099
  - risk analysis
    - qualitative, 72, 76-78
    - quantitative, 72-76, 78-79
    - software security, 1144-1145
  - risk assessment
    - approaches, 72-76
    - asset valuation, 65-66
    - business impact analysis, 109-112
    - methodologies, 67-72
    - monitoring risk, 91-96
  - overview, 63-64
  - preventive and detective measures, 944
  - responses. See risk responses
  - SDLC, 1082-1083
  - teams, 66-67
  - risk-based access control, 775-776
  - risk-level acceptance in SDLC, 1082
  - risk management
    - assessment. See risk assessment
    - business continuity. See business continuity (BC)
    - chapter questions, 118-123
    - chapter review, 116-118
    - concepts, 53-54
    - holistic, 54-55
    - information systems risk management
      - policy, 56
      - overview, 53
      - process, 57-58
      - risk analysis, 72-79
      - supply chain, 96-101
      - teams, 56-57
      - threats, 60-63
      - vulnerabilities, 58-60, 62-63
    - Risk Management Framework, 172-177
    - risk responses
      - control assessments, 88-91
      - control types, 83-88
      - countermeasure selection and implementation, 81-83
      - overview, 79-80
      - risk management response, 57
      - total risk vs. residual risk, 81
    - Rivest, Ron, 340, 352
    - roaming 802.11f standard, 574

- robustness of security metrics, 854
- role-based access control (RBAC) model, 771
  - characteristics, 776
  - core, 772
  - hierarchical, 772-773
  - roles and responsibilities
- data, 244-245
- definitions, 799
- incident response plans, 1000-1002
- organizational. See organizational roles and responsibilities
- separation of duties, 394
- software development, 1080
- tasks and responsibilities, 886

#### ▲CISSP All-in-One Exam Guide

1304

- rollback plans, 905
- rolling hot sites, 1049
- root account, 859
- round-trip time (RTT) in latency, 654
- route flapping, 535
- routers
  - vs. bridges, 657
- characteristics, 665
- overview, 660-662
- Routing Information Protocol (RIP), 535
- routing policies in BGP, 537
- routing protocols
  - attacks, 537
- autonomous systems, 533-534
- distance-vector vs. link-state, 535
- dynamic vs. static, 534-535
- exterior, 536-537
- interior, 535-536
- RPC security (RPCSEC), 704
- RPCs (remote procedure calls), 703-704
- RPO (recovery point objective)
  - disaster recovery, 1031-1032
- high availability, 1052
- RSA algorithm, 340-342
- RSA-CRT (Chinese Remainder Theorem), 372
- RSA SecurID, 730-732
- RTCP (RTP Control Protocol), 691
- RTEs (runtime environments), 1122-1124
- RT0 (recovery time objective)
  - disaster recovery, 1031-1033
- high availability, 1052
- RTP Control Protocol (RTCP), 691
- RTP (Real-time Transport Protocol), 689, 691
- RTT (round-trip time) in latency, 654



- RTUs (remote terminal units)
- DNP3, 626
- industrial controls, 290
- SCADA systems, 294
- Ruff, Howard, 1029
- rule-based access control (RB-RBAC), 774
- rule-based IDS/IPS, 967
- rules in PKI key management, 366–367
- RUM (real user monitoring) vs. synthetic transactions, 832
- runbooks for incidents, 1006
- runtime environments (RTEs), 1122–1124

## S

- S/MIME (Secure MIME), 626
- SaaS (Software as a Service), 228, 302–303
- SABSA (Sherwood Applied Business Security Architecture), 14–15, 173
- SACs (single-attached concentrators) in FDDI, 498
- Safe Harbor Privacy Principles, 143
- “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” 140
- safes, 221–222
- safety issues
  - disaster recovery, 1059
  - fires, 454.–457
  - personnel. See personnel safety and security
  - sags in electric power, 451
  - salvage teams in disaster recovery plans, 1056
- SAML (Security Assertion Markup Language), 779–780
- SAMM (Software Assurance Maturity Model), 1109–1110
- sandboxes
  - antimalware, 969–970, 972–973
  - Java Virtual Machine, 1123
  - sanitized media, 259
- Sarbanes-Oxley Act (SOX), 20
- SAs (security associations) in IPSec, 608
- SASL (Simple Authentication and Security Layer), 624
- SASs (single-attachment stations) in FDDI, 498
- SAST (static application security testing), 1139
- satellite communications, 589–590
- SCADA (supervisory control and data acquisition) systems, 290, 294
- scalability
  - Kerberos, 785
  - packet-filtering firewalls, 948
  - stateful firewalls, 952

- scans
  - devices, 226
  - facial, 728
  - iris, 727
  - palm, 727
  - retina, 727
  - software vulnerabilities, 901

## ▲Index

- 1305
- scenarios for backups, 863
- schemes in URLs, 613
- Schneier, Bruce, 385
- Scientific Working Group on Digital Evidence (SWGDE), 1009
- SCIFs (sensitive compartmented information facilities), 443
- SCM (software configuration management), 1142
- scope creep in project management, 1081
- scope of audits, 839
- scope values in OIDS, 784
- scoping controls, 258
- SCPs (service control points), 683
- screen sharing in meeting applications, 694
- screened host firewalls,
  - 959-960, 963
- screened subnet firewalls, 960-962
- screening candidates, 35-36
- screens in information access control, 801
- script kiddies, 60, 135
- scrubbing logs, 744
- Scrum methodology, 1101-1102
- scytale ciphers, 318
- SD-WAN (software-defined wide area networking), 635
- SDLC. See software development life cycle (SDLC)
- SDN. See software-defined networking (SDN)
- sealing systems, 405
- second-generation (2G) mobile wireless, 585-586
- second-generation programming languages, 1118
- secondary storage in information access control, 801
- SecOps, 887
- secret algorithms vs. public, 369
- secret classification level, 216-218
- secret keys
  - hybrid methods, 348
  - RSA, 340-341

- symmetric key cryptography, 329
- secure defaults
- network security, 598
- third-party connectivity, 706
- web services, 611

- secure design principles, 390
- defaults, 396
- defense in depth, 390–391
- failing securely, 396–397
- least privilege, 394–395
- privacy by design, 397
- separation of duties, 393–394
- shared responsibility, 392–393
- simplicity, 395–396
- trust but verify, 392
- zero trust, 392
- secure enclaves in trusted execution environments, 408
- Secure Hash Algorithm (SHA)
  - description, 352
  - passwords, 722
- Secure MIME (S/MIME), 626
- Secure Shell (SSH)
  - code repositories, 1144
  - communications channels, 701–702
- secure software
  - acquired software, 1145–1148
- APIs, 1132
- application security testing, 1139–1140
- assemblers, compilers, and interpreters, 1120–1122
- assessments, 1144–1145
- change management, 1145
- chapter questions, 1150–1153
- chapter review, 1148–1150
- code repositories, 1143–1144
- cohesion and coupling, 1130–1132
- configuration management, 1142
- continuous integration and delivery, 1140–1141
- controls, 1136–1144
- development platforms, 1137–1138
- libraries, 1132–1133
- object-oriented programming, 1124–1130
- overview, 1117
- programming languages and concepts, 1117–1120
- risk analysis and mitigation, 1144–1145
- runtime environments, 1122–1124
- secure coding practices, 1134–1136
- SOAR, 1141–1142
- source code vulnerabilities, 1133–1134
- tool sets, 1138

1306

security

aligning to business strategy, 13-16

assessments. See assessments

endpoint, 673-674

network. See network security

policies, 27-29

vs. privacy, 21

security administrators, 24

security architects, tasks and responsibilities, 886

security architectures, 385

chapter questions, 413-416

chapter review, 411-413

encryption locations, 411

information systems, 404-410

secure design principles, 390-397

security models, 397-404

security requirements, 404

threat modeling, 385-390

Security Assertion Markup Language (SAML), 779-780

security associations (SAs) in IPSec, 608

security champions, 43

security controls. See controls

security directors, tasks and responsibilities, 886

security effectiveness in control assessments, 90-91

security film windows, 441

security information and event management (SIEM) systems  
event data, 831

forensics investigations, 1021

incidents, 990-991

logs, 744, 979-980

security operations centers, 940

security managers, tasks and responsibilities, 886

security models

Bell-LaPadula, 398-399

Biba, 399-400

Brewer and Nash, 402

Clark-Wilson, 400

Graham-Denning, 402

Harrison-Ruzzo-Ullman, 402-404

noninterference, 400-401

overview, 397-398

summary, 403

security operations, 939

- antimalware software, 969–972
- artificial intelligence tools, 976–978
- chapter questions, 984–988
- chapter review, 982–984
- firewalls. *See* firewalls
- honeypots and honeynets, 974–976
- intrusion detection and prevention systems
- overview, 967–969
- logging and monitoring, 978–982
- outsourced security services, 973–974
- preventive and detective measures overview, 944–945
- sandboxes, 972–973
- security operations centers, 939–943
- security operations centers (SOCs)
- cyberthreat hunting, 943
- elements, 940–941
- overview, 939
- threat data sources, 942–943
- threat intelligence, 941–942
- security operations management, 885
- accountability, 887–888
- change management, 891–893
- chapter questions, 934–938
- chapter review, 932–934
- configuration management, 893–895
- foundational concepts overview, 885–887
- job rotation, 889–890
- need-to-know and least privilege, 888
- patch management, 903–906
- personnel safety and security, 929–932
- physical security. *See* physical security and controls
- privileged account management, 889
- resource protection, 895–899
- separation of duties and responsibilities, 888–889
- service level agreements, 890
- vulnerability management, 900–903
- security orchestration, automation, and response (SOAR) platform
- components, 980
- secure software, 1141–1142
- security programs in frameworks, 172, 180–183
- Security Safeguards Principle in OECD, 142
- security zones in CPTED, 429–430

## ▲Index

1307

- SecY (MACSec Security Entity), 501
- SEDs (self-encrypting drives), 407
- segmentation, network, 295, 703

- segments in TCP, 509
- SEI (Software Engineering Institute), 993
- select step in Risk Management Framework, 175
- self-encrypting drives (SEDs), 407
- self-healing SONENTs, 539
- self-service
  - password resets, 737
  - profile updates, 740
- Sender Policy Framework (SPF), 624
- senior management, awareness
- programs for, 41-42
- sensitive classification level, 216-217
- sensitive compartmented information facilities (SCIFs), 443
- sensitive data
  - classification, 215
  - data loss prevention, 266, 270
- sensors in incident detection, 995-996
- separation of duties (SoD) principle
  - network security, 599
  - overview, 888-889
  - purpose, 34
  - role-based access control, 773
- security architectures, 393-394
- site and facility security, 421
- software development, 1090
- third-party connectivity, 706
- web services, 612
- sequels for tabletop exercises, 1063
- sequence numbers in TCP, 508
- server-based systems, 284-285
- serverless systems, 299-301
- servers
  - clustered, 1051
- OAuth, 782
- proxy, 663-664
- service availability risk from unmanaged patching threats, 904
- service bureaus in disaster recovery, 1045
- service control points (SCPs), 683
- service level agreements (SLAs)
  - high availability, 1050
- overview, 890
- supply chain risk management, 101
- service-oriented architecture (SOA)
  - description, 780-781
  - web services, 612-613
- Service Provisioning Markup Language (SPML), 777-779
- Service Set IDs (SSIDs), 565
- services in supply chain risk management, 99
- Session Initiation Protocol (SIP), 689-691

- session keys, 349–350
- session layer
  - functions and protocols, 484
- OSI model, 477–478
- session management, 740–741
- severity levels for incidents, 1003
- SGML (Standard Generalized Markup Language), 776
- SHA (Secure Hash Algorithm)
  - description, 352
- passwords, 722
- shallow depth of focus in CCTV systems, 915
- Shamir, Adi, 340
- Shannon, Claude, 332
- shared key authentication (SKA), 575
- shared portions in objects, 1128
- shared responsibility principle
  - network security, 599
- security design, 392–393
- site and facility security, 420–421
- third-party connectivity, 706
- web services, 612
- shareware, 153
- sharing data, 238–239
- Shedd, William G.T., 53
- Sherwood Applied Business Security Architecture (SABSA), 14–15, 173
- shielded twisted pair (STP) cable, 649
- Shkreli, Martin, 20
- Shortest Path Bridging (SPB) protocol, 657
- shoulder surfing, 5
- side-channel attacks
  - cryptography, 371–372
  - description, 257
- smart cards, 734–735
- SIEM systems. See security information and event management (SIEM) systems
- signal switching points (SSPs), 682
- signal transfer points (STPs), 683
- Signaling System 7 (SS7) protocol, 682

## ▲ CISSP All-in-One Exam Guide

1308

- signature-based detection in antimalware software, 969, 971
- signature dynamics, 727–728
- signatures in antimalware software, 969
- Simple Authentication and Security Layer (SASL), 624
- simple integrity axiom in Biba model, 399
- Simple Mail Transfer Protocol (SMTP), 622
- Simple Network Management Protocol (SNMP), 522–524

- Simple Object Access Protocol (SOAP), 614–615, 780
- simple security rule in Bell-LaPadula, 398
- simplex communication, 831
- simplex mode in session layer, 478
- simplicity
  - network security, 599
  - secure design principles, 395–396
  - security metrics, 854
  - site and facility security, 422
  - third-party connectivity, 706
- Simpson, O.J., 129–130
- simulation tests in disaster recovery plans, 1064
- simulations for breach attacks, 828
- single-attached concentrators (SACs) in FDDI, 498
- single-attachment stations (SASs) in FDDI, 498
- single loss expectancy (SLE) key risk indicators, 857
- quantitative risk analysis, 73–75
- single mode in fiber-optic cable, 651
- single sign-on (SSO) identity management, 750–752
- replay attacks, 372–373
- SIP (Session Initiation Protocol), 689–691
- site and facility security
  - access control, 802–803
  - backups, 1040–1041
  - chapter questions, 463–465
  - chapter review, 461–462
  - controls. See controls for site and facilities
  - CPTED, 427–433
  - defaults, 422
  - defense in depth, 419
  - design overview, 417–418
  - least privilege, 421
- locks, 917–923
- overview, 417, 916–917
- physical security programs, 433–441
- planning steps, 423–427
- principles, 418–423
- privacy by design, 423
- separation of duties, 421
- shared responsibility, 420–421
- simplicity, 422
- threat modeling, 418–419
- trust but verify, 420
- zero trust, 419–420
- Site Security Design Guide, 906
- situational awareness, 744
- 6to4 tunneling method, 514



- Six Sigma methodology, 197
- SKA (shared key authentication), 575
- Slack service, 1057
- SLAs (service level agreements)
  - high availability, 1050
  - overview, 890
  - supply chain risk management, 101
- SLE (single loss expectancy)
  - key risk indicators, 857
  - quantitative risk analysis, 73–75
- slot locks, 921
- smart cards
  - access codes, 921
  - attacks on, 734–735
  - ownership-based authentication, 733–735
- smart phones, 688
- smoke-activated fire suppression, 456
- smoke detectors, 445
- SMTP (Simple Mail Transfer Protocol), 622
- Smyth, Robin, 20
- SNMP (Simple Network Management Protocol), 522–524
- snooping in DHCP, 519
- Snowden, Edward, 62
- SOA (service-oriented architecture)
  - description, 780–781
  - web services, 612–613
- SOAP (Simple Object Access Protocol), 614–615, 780
- SOAR (security orchestration, automation, and response) platform
  - components, 980
- secure software, 1141–1142

## ▲Index

- 1309
- social engineering
  - awareness programs, 42
  - cryptography attacks, 375
  - description, 5, 60
  - human vulnerabilities, 902–903
  - passwords, 721
  - training, 864–865
  - social network vulnerabilities, 60
- sockets
  - description, 504
  - network, 703
- SOCKS proxy firewalls, 956
- SOCs. See security operations centers (SOCs)
- SoD principle. See separation of duties (SoD) principle
- soft controls for risk responses, 83

- soft tokens in one-time passwords, 732
- software
  - antimalware, 969–972
  - backups in business continuity planning, 1070
  - cryptography systems, 602
  - escrow, 1070, 1143
  - licensing, 226
  - meeting applications, 695
  - piracy, 153–154
  - secure. See secure software
  - smart card attacks, 735
  - supply chain risk management, 99
  - tracking, 224–227
  - vulnerabilities, 901
- Software as a Service (SaaS), 228, 302–303
- Software Assurance Maturity Model (SAMM), 1109–1110
- software configuration management (SCM), 1142
- software-defined networking (SDN)
  - approaches, 634–635
  - control and forwarding planes, 633–634
  - overview, 632–633
  - secure software, 1136
  - software-defined security (SDS), 1136
  - software-defined wide area networking (SD-WAN), 635
  - software developers, tasks and responsibilities, 886
- software development
  - Agile methodologies, 1100–1103
  - chapter questions, 1112–1116
  - chapter review, 1110–1111
  - cleanroom methodology, 1105
  - DevOps, 1103–1104
  - DevSecOps, 1104
  - exploratory methodology, 1104
  - Incremental methodology, 1096–1097
  - Joint Application Development methodology, 1104
  - maturity models, 1106–1110
  - methodologies overview, 1095
  - methodologies summary, 1106
  - overview, 1079
  - prototypes, 1096
  - Rapid Application Development methodology, 1099–1100
  - reuse methodology, 1105
  - roles, 1080
  - SDLC. See software development life cycle (SDLC)

- Spiral methodology, 1098-1099
- Waterfall methodology, 1095-1096
- software development life cycle (SDLC)
  - design phase, 1083-1087
  - development phase, 1087-1089
  - operations and maintenance phase, 1091-1094
  - overview, 1079-1080
  - phases summary, 1094
  - project management, 1081
  - requirements gathering phase, 1082-1083
  - testing phase, 1089-1091
- Software Engineering Institute (SEI), 993
- software engineers, 1080
- software guard in MAC, 770
- Software Requirements Specification (SRS), 1083
- solar window film windows, 441
- solid-core doors, 440
- something a person does authentication factor, 718
- something a person has authentication factor, 718-719
- something a person is authentication factor, 718
- something a person knows authentication factor, 718

#### ▲CISSP All-in-One Exam Guide

- 1310
- somewhere a person is authentication factor, 718
- SONETs (Synchronous Optical Networks), 538-539
- source code analysis attacks
  - in cryptography, 370
- source code vulnerabilities, 1133-1134
- source files, protecting, 896
- source routing in firewalls, 966
- Soviet Union collapse, increase of attacks from, 134
- SOW (statements of work) in project management, 1081
- SOX (Sarbanes-Oxley Act), 20
- Spafford, Eugene H., 3
- spaghetti code, 1126
- Spanning Tree Protocol (STP), 657
- SPB (Shortest Path Bridging) protocol, 657
- spearphishing, 865
- Specht, Paul, 150
- special characters in passwords, 720
- Spectre attacks, 257, 372
- speed
  - biometric authentication, 726

- TCP vs. UDP, 506
- SPF (Sender Policy Framework), 624
- spikes in electric power, 451
- Spiral methodology for software development, 1098–1099
- split knowledge, 34
- split tunnels in VPNs, 697
- splitting DNS, 530
- Splunk product, 979
- SPML (Service Provisioning Markup Language), 777–779
- spoofing
  - e-mail, 623
- firewalls, 965
- STRIDE model, 388
- spread spectrum wireless communications, 561–563
- sprinklers, 459–460
- sprints in Scrum methodology, 1102
- SRKs (storage root keys) in Trusted Platform Modules, 405
- SRS (Software Requirements Specification), 1083
- SS7 (Signaling System 7) protocol, 682
  
- SSD (static separation of duty) relations in RBAC, 773
- SSH (Secure Shell)
  - code repositories, 1144
  - communications channels, 701–702
- SSIDs (Service Set IDs), 565
- SSO (single sign-on)
  - identity management, 750–752
- replay attacks, 372–373
- SSPs (signal switching points), 682
- staff, awareness programs for, 42
- stakeholders
  - enterprise architecture frameworks, 190
  - incident notifications, 1004
  - standalone mode in WLANs, 565
  - standard changes, 892
- Standard Generalized Markup Language (SGML), 776
- standard windows, 441
- standards
  - business continuity, 104–106
  - coding, 1135–1136
  - controls, 258
  - industry, 156–158
  - logs, 979
  - organizational, 29–31
  - WLANs, 565–574
- standby lighting, 912
- standby UPS systems, 453

- star integrity axiom in Biba model, 399
- star property rule in Bell-LaPadula, 398
- star topology, 488
- start bits, 646
- state actors, 60–61
- state tables
- stateful firewalls, 949, 952
- three-way-handshake process, 951
- stateful firewalls, 949–952
- stateful NAT, 533
- stateless inspection in packet-filtering firewalls, 948
- statements of work (SOW) in project management, 1081
- states
  - controls, 254–258
  - TCP connections, 951
- static analysis
  - antimalware software, 970
  - application security, 1139

## ▲Index

1311

- static application security testing (SAST), 1139
- static electricity, 454
- static mapping in NAT, 532
- static routing protocols, 534–535
- static separation of duty (SSD) relations in RBAC, 773
- statistical attacks in cryptography, 370
- statistical time-division multiplexing (STDM), 544
- steganography, 264–265
- stegomedium, 265
- Stevens, Ted, 469
- sticky notes in Kanban methodology, 1102–1103
- Stoll, Clifford, 643
- stop bits, 646
- storage, data, 232–233, 259–260
- storage facilities, 447–448
- storage keys in Trusted Platform Modules, 406
- storage root keys (SRKs) in Trusted Platform Modules, 405
- STP (shielded twisted pair) cable, 649
- STP (Spanning Tree Protocol), 657
- STPs (signal transfer points), 683
- strata in NTP, 831
- strategic alignment, 15–16
- stream ciphers in symmetric key cryptography, 333–334
- stream-symmetric ciphers, 575

- streaming protocols, 691
- strict liability category in civil law, 128
- STRIDE model, 387–388
- strong authentication, 718–719
- strong star property rule in Bell-LaPadula, 398
- structured walkthrough tests in disaster recovery plans, 1063
- subjects
  - ABAC, 774
  - data, 245
- subnet masks in IP addresses, 511–512
- subnets in IP addresses, 510–512
- substitution ciphers, 318
- sub-techniques in MITRE ATT&CK framework, 389
- succession planning, 1043
- Sullivan, Joseph, 20
- supernetting IP addresses, 512
  
- supervisor role, 24
- supervisory control and data acquisition (SCADA) systems, 290, 294
- supply chain risk management
  - attacks, 133
  - hardware, 98
  - minimum security requirements, 100
  - overview, 96–98
  - risk sources, 99–100
  - service level agreements, 101
  - services, 99
  - software, 99
  - upstream and downstream, 98
- supply system threats in site planning, 423
- support agreements, 672
- support staff, tasks and responsibilities, 886
- surges in electric power, 451
- surveillance
  - CPTED, 431–432
  - description, 913
- digital forensics, 1019–1020
- suspending accounts, 860
- sustain stage in change management, 892
- Sutter Health of California breach, 255
- SVCs (switched virtual circuits), 549
- SWGDE (Scientific Working Group on Digital Evidence), 1009
- swipe cards for ownership-based authentication, 732–733
- switch controls in device locks, 921
- switch spoofing attacks, 632
- switched virtual circuits (SVCs), 549
- switches
  - characteristics, 665
  - layer 3 and 4, 659

- overview, 657-658
- VLANs, 630
- switching WANs, 545-547
- symbolic AI approach, 976-978
- symbolic links, 819, 821
- symmetric key cryptography
  - with asymmetric, 346-349
- block ciphers, 330-333
  - description, 328
- initialization vectors, 334-335
- overview, 329-330
- stream ciphers, 333-334
- summary, 330

#### ▲CISSP All-in-One Exam Guide

- 1312
- symmetric services in DSL, 684
- SYN/ACK packets, 508
- SYN floods, 508
- SYN packets, 508, 949-951
- SYN-RECEIVED state in TCP connections, 951
- SYN-SENT state in TCP connections, 951
- synchronization
  - NTP, 830
- passwords, 737
- Synchronous Optical Networks (SONETs), 538-539
- synchronous replication, 1039
- synchronous token devices for one-time passwords, 730-731
- synchronous transmission, 645-647
- synthetic transactions, 832
- system access control, 802
- system account access review, 798
- system administrators, tasks and responsibilities, 886
- system architectures
  - chapter questions, 311-315
  - chapter review, 310-311
- client-based, 284
- cloud-based, 301-305
- database, 285-286
- distributed, 307-309
- high-performance computing, 288-289
- industrial control systems, 289-296
- overview, 283
- pervasive, 305-307
- server-based, 284-285
- virtualized systems, 296-301
- system authentication, 579
- system images, 896
- system-level event audits, 742
- system owners, 23-24

- system resilience in availability, 1051
- system sensing access control readers, 925
- system-specific controls in Risk Management Framework, 175
- system-specific policies, 29
- system testing, 818

## T

- T-carriers for WANs, 541-542

### tables

- forwarding, 656-657

- rainbow, 721-722

- stateful firewalls, 949, 952

- three-way-handshake process, 951

- tabletop exercises (TTXs) in disaster recovery plans, 1063-1064

- TACACS (Terminal Access Controller Access Control System), 790-793

- TACS (Total Access Communication System), 584

- tactics in MITRE ATT&CK framework, 389

- tailoring controls, 258

- tamper-resistant property in reference monitors, 766

- tampering category in STRIDE model, 388

- tape vaulting for backups, 1039

- tapes for backups, 860

- Target company breach, 96-97

- target hardening vs. CPTED, 428

- targeted penetration tests, 826-827

- targets of attacks, 474

- tar pits, 976

- taxonomies in data retention, 236

- TCG (Trusted Computing Group), 404

- TCP. See Transmission Control Protocol (TCP)

- TCP/IP (Transmission Control Protocol/Internet Protocol) suite, 471, 502-503

- TDF (transborder data flow), 146-147

- TDM (time-division multiplexing), 541-542

- TDMA (time division multiple access)

- GTS, 570

- mobile communications, 584

### teams

- backup administrators, 1035

- business continuity planning, 1030

- disaster recovery plans, 1056

- incident response, 991, 1000-1001

- risk analysis, 76, 78

- risk assessment, 66-67

- risk management, 56-57

- software development, 1080

- technical controls



- assessments. See testing
- risk responses, 83, 86–87
- technical reports, 872–873
- technical sensors in incident detection, 995
- technological communication protocols, 646
- TEEs (trusted execution environments), 408–411
- telephone calls in PBXs, 665–667

## ▲Index

1313

- Telephone Records and Privacy Protection Act, 865
- telephones in disaster recovery plans, 1062
- telepresence in meeting applications, 695
- temperature
  - data processing facilities, 446
  - HVAC systems, 453–454
  - tempered windows, 441
- templates for disaster recovery plans, 1059
- Temporal Key Integrity Protocol (TKIP), 577–578
- Teredo tunneling, 514
- Terminal Access Controller Access Control System (TACACS), 790–793
- terminals in H.323, 689
- termination processes in personnel security, 37–38
- territorial reinforcement in CPTED, 431–432
- tertiary sites in disaster recovery, 1046
- Tesla, Nikola, 559
- test coverage, 837
- test-driven development
  - Extreme Programming, 1102
  - software development, 1089
- testing
  - application security, 1139–1140
  - backups, 863
  - code reviews, 833–834
  - code testing, 834–835
  - compliance checks, 838
  - data loss prevention, 270–271
  - disaster recovery goals, 1054
  - disaster recovery plans, 1061–1065
  - federated identity, 755
  - interface, 837
  - log reviews, 828–831
  - misuse cases, 835–836
  - overview, 817
  - penetration, 822–827
  - red teaming, 827–828
  - SDLC, 1080, 1089–1091

- Spiral methodology, 1098
- strategies, 813–816
- synthetic transactions, 832
- test coverage, 837
- vulnerabilities, 817–822
- testing mode in anomaly-based IDS/IPS, 967
- text messages in disaster recovery plans, 1056
  
- TGSs (ticket granting services) in KDC, 785–786
- Thailand, Personal Data Protection Act in, 144
- The Onion Router (TOR), 307
- The Open Group Architecture Framework (TOGAF), 172, 194–195
- The Silk Road, 665
- thermal relocking function in safes, 222
- third-generation (3G) mobile wireless, 585–586
- Third Generation Partnership Project (3GPP), 586
- third-generation programming languages, 1118–1119
- third parties
  - audits, 843–844
  - business continuity planning, 1068
  - connectivity, 705–706
  - dealing with, 39
  - security provided by, 973–974
  - software escrow, 1143
  - software security, 1147
  - third-party sensors in incident detection, 995
  - third-party services, federated identity with, 754–756
- threat data sources for security operations centers, 942–943
- Threat Dragon, 1087
- threat hunters, tasks and responsibilities, 886
- threat hunting in security operations centers, 943
- threat intelligence analysts on incident response teams, 1001
- threat intelligence in security operations centers, 941–942
- threat modeling
  - attack trees, 386–387
- Cyber Kill Chain, 387–389
  - importance, 389–390
- MITRE ATT&CK framework, 389
- network security, 598
- overview, 385
- site and facility security, 418–419
- software development design, 1086
- STRIDE, 387–388
- third-party connectivity, 705

threat trees in software development  
design, 1086  
threat working group (TWG), 92

#### ▲CISSP All-in-One Exam Guide

1314  
threats  
  cybercriminals, 60  
  defined, 8  
  duress, 931-932  
  hacktivists, 61  
  identifying, 62-63  
  internal actors, 61-62  
  nation-state actors, 60-61  
  nature, 62  
  overview, 58  
  site planning, 423  
  three-factor authentication, 719  
  three-way-handshake process  
  SIP, 689  
  TCP, 949-951  
  throughput in cabling, 654-655  
  thunking, 296  
  ticket granting services (TGSs) in KDC,  
  785-786  
  tickets in KDC, 785-788  
  Tier 1 (organization view) in risk  
  management, 55  
  Tier 2 (mission/business process view) in risk  
  management, 55  
  tiers  
  Cybersecurity Framework, 182  
  risk management, 55  
  tight coupling software, 1131-1132  
  time division multiple access (TDMA)  
  GTS, 570  
  mobile communications, 584  
  time-division multiplexing (TDM), 541-542  
  time-limited trials for third-party  
  software, 1147  
  time-of-check to time-of-use (TOC/TOU)  
  in atomic execution, 410  
  time to first byte (TTFB) in latency, 654  
  Time to Live (TTL) values in packets, 512  
  TIME-WAIT state in TCP connections, 951  
  timely characteristic in threat intelligence, 941  
  timeouts in session termination, 741  
  timing attacks in cryptography, 371-372  
  timing smart cards, 735  
  TKIP (Temporal Key Integrity Protocol),  
  577-578  
  TLS. See Transport Layer Security (TLS)  
  TOC/TOU (time-of-check to time-of-use)

in atomic execution, 410

TOGAF (The Open Group Architecture Framework), 172, 194–195

token passing, 491–492

Token Ring, 495–496, 499

tokens

electronic access control, 925

one-time passwords, 730

toll fraud

IP telephony, 692

PBX systems, 666

tool sets for secure software, 1138

top-down approach in security programs, 199

top-level domains in DNS, 527

top secret classification level, 216–218

topologies for local area networks, 487–490

Tor network, 665

TOR (The Onion Router), 307

tort law system, 127–129

Total Access Communication

System (TACS), 584

total risk vs. residual risk, 81

TPC (Transmit Power Control), 574

TPMs (Trusted Platform Modules), 404–406

TPs (transformation procedures)

in Clark-Wilson model, 400

Traceroute tool, 520–522

tracking

digital asset management, 261–262

hardware, 224

software, 224–227

trade secrets, 148–149

trademarks, 150

traffic direction in packet-filtering firewalls, 948

traffic-flow security, 601

traffic shaping in QoS, 551

trailer hot sites, 1049

training, 40

artificial intelligence tools, 977–978

content reviews, 43

degrees and certifications, 40–41

disaster recovery communications, 1057

disaster recovery plans, 1060–1061,  
1064–1065

evaluating, 43–44

incident response, 993

measuring security, 863–867

methods and techniques, 41–43

personnel, 930–931

▲Index

- training mode in anomaly-based IDS/IPS, 967
- transactions, synthetic, 832
- transborder data flow (TDF), 146–147
- transfer risk strategy
  - ISO/IEC 27005, 178
- overview, 79
- transfers in personnel security, 37–38
- transformation procedures (TPs)
  - in Clark-Wilson model, 400
- Transmission Control Protocol (TCP)
  - connection-oriented protocol, 479
  - data structures, 509
  - handshakes, 508, 949–951
  - transport layer, 479, 503
  - vs, UDP, 503–506
- Transmission Control Protocol/Internet Protocol (TCP/IP) suite, 471, 502–503
- transmission media
  - cabling, 648–655
  - overview, 643–644
  - types, 644–648
- transmission methods for local area networks, 499–500
- Transmit Power Control (TPC), 574
- transparent bridging, 656–657
- transponders, 925
- transport adjacency in IPSec, 609
- transport layer
  - functions and protocols, 484
- OSI model, 479–480
- Transport Layer Security (TLS)
  - data in motion, 255–256
  - malware using, 604–605
  - network security, 602–605
  - suites, 603–604
  - types, 610–611
- transport supplies in forensics field kits, 1015
- transposition ciphers, 318
- travel safety, 930
- tree topology, 488
- trials for third-party software, 1147
- trialware, 153
- TrickBot Trojan, 604, 969
- Trojans in TLS, 604
- trust but verify principle
  - network security, 599
  - secure architectures, 392
- site and facility security, 420
- third-party connectivity, 706
- web services, 612
- Trust Centers for mobile communications, 572
- trust in federated identity, 755

- Trusted Computing Group (TCG), 404
- trusted execution environments (TEEs), 408–411
- Trusted Platform Modules (TPMs), 404–406
- TTFB (time to first byte) in latency, 654
- TTL (Time to Live) values in packets, 512
- TTXs (tabletop exercises) in disaster recovery plans, 1063–1064
- tumbler locks, 918
- tuning data loss prevention, 270–271
- tunnels
  - DNS, 619
  - ICMP, 520
  - IPv6, 514–515
  - TLS, 610
- turnstiles, 441
- Tuzman, Kaleil Isaza, 20
- TWG (threat working group), 92
- twisted-pair cabling, 649–650
- two-factor authentication (2FA), 719
- type 1 hypervisors in virtual machines, 297
- type 2 hypervisors in virtual machines, 297
- Type I errors in biometric authentication, 724–725
- Type II errors in biometric authentication, 724–725
- types in incidents classification, 1002

## U

- U.S. Patent and Trademark Office (USPTO), 150
- UAC (User Agent Client) in SIP, 689
- UAS (User Agent Server) in SIP, 689
- ubiquitous computing, 305
- UBR (unspecified bit rate) in ATM, 551
- UC (unified communications), 695–696
- UCDs (use case diagrams) in software development, 1083
- UDIs (unconstrained data items) in ClarkWilson model, 400
- UDP. See User Datagram Protocol (UDP)
- UEBA (user and entity behavior analytics), 981

## ▲CISSP All-in-One Exam Guide

1316

- UEM (unified endpoint management) systems, 226
- UML (Unified Modeling Language) software development, 1083
- use case diagrams, 835–836
- uncertainty in risk assessment, 74
- unclassified classification level, 216–218
- unconstrained data items (UDIs)

- in Clark-Wilson model, 400
- undercover investigations in digital forensics, 1020
- understanding factor in outsourced security services, 974
- unicast transmission method, 499
- unified communications (UC), 695–696
- unified endpoint management (UEM) systems, 226
- Unified Modeling Language (UML) software development, 1083
- use case diagrams, 835–836
- uniform resource identifiers (URIs) for web services, 613–614
- uniform resource locators (URLs) in DNS, 524, 531
- uninterruptible power supplies (UPSs) data processing facilities, 446
- online, 452–453
- standby, 453
- unit testing in software development, 1089, 1091
- United States laws for data breaches, 141–142
- unmanaged patching, 904–905
- unshielded twisted pair (UTP) cable, 649–650
- unspecified bit rate (UBR) in ATM, 551
- updates
  - Internet of Things, 307
  - profiles, 740
- UPS Brown color, 150
- UPSs (uninterruptible power supplies) data processing facilities, 446
- online, 452–453
- standby, 453
- upstream suppliers in risk management, 98
- uptime in high availability, 1050
- urgency in incidents classification, 1002
- URIs (uniform resource identifiers) for web services, 613–614
- URLs (uniform resource locators) in DNS, 524, 531
- usage in TCP vs. UDP, 506
- use case diagrams (UCDs) in software development, 1083
- use cases
  - data loss prevention, 271
  - misuse case testing, 835–836
- Use Limitation Principle in OECD, 142
- user access review for identity and access, 797
- user-activated readers, 925
- User Agent Client (UAC) in SIP, 689
- User Agent Server (UAS) in SIP, 689
- user and entity behavior analytics (UEBA), 981

- user data file backups, 861
- User Datagram Protocol (UDP)
  - connectionless protocol, 479
- connections, 951–952
- vs. TCP, 503–506
- transport layer, 479
- user-level event audits, 743
- user managers, 24
- user stories in Agile methodologies, 1101
- users
  - Clark-Wilson model, 400
  - description, 25
  - provisioning, 739
- USPTO (U.S. Patent and Trademark Office), 150
- utilities
  - electric power, 448–453
  - HVAC, 453–454
  - water and wastewater, 448–450
- utility tunnels in physical security, 439
- UTP (unshielded twisted pair) cable, 649–650

## V

- vacations, mandatory, 35, 890
- Valasek, Chris, 627
- validation
  - assessments, 815–816
  - parameters, 1132
  - risk controls, 90
  - software development, 1090
- Validation practice in Good Practice Guidelines, 106
- valuation of assets, 65–66
- variable bit rate (VBR) in ATM, 551
- vaulting for backups, 1038–1039
- vaults, protecting, 222

## ▲Index

1317

- VBR (variable bit rate) in ATM, 551
- VDI (virtual desktop infrastructure), 700–701
- VDSL (very high-data-rate DSL), 684
- vendors, 39
- ventilation ducts in physical security, 439
- Veracode report, 1133
- verifiable property for reference monitors, 766
- verification
  - backups, 860–862
  - message integrity, 354–358
  - risk controls, 90
  - software development, 1090
  - supply chain risk management, 100
  - verification 1:1, 718



- Verification function in SAMM, 1109
- Vernam, Gilbert, 325
- Vernam cipher, 325–328
- versatile memory in Trusted Platform Modules, 406
- versioning software, 1142–1144
- vertical enactment for privacy, 147
- very high-data-rate DSL (VDSL), 684
- very high-level programming languages, 1119–1120
- very small aperture terminals (VSATs), 589–590
- vibration detectors, 927
- VIDs (VLAN identifiers), 631
- views in enterprise architecture frameworks, 190, 192
- Vigenère, Blaise de, 319
- Vigenère cipher, 319
- violence, threats of, 931–932
- virtual circuits in WANs, 548–549
- virtual desktop infrastructure (VDI), 700–701
- virtual directories, 750
- Virtual eXtensible Local Area Networks (VxLANs), 632
- virtual firewalls, 964
- virtual local area networks (VLANs) latency, 654
- overview, 630–632
- virtual machines (VMs), 296, 704–705
  - antimalware, 969–970
  - benefits, 297–298
  - hypervisors, 297
  - third-party connectivity, 705
- Virtual Network Computing (VNC), 700
- virtual NICs (vNICs), 704–705
- virtual passwords, 723
- virtual private clouds (VPCs), 301
- virtual private networks (VPNs) authentication protocols, 697–699
- data in motion, 256
- IPSec, 607–609
- L2TP, 606–607
- overview, 605, 697
- PPTP, 606
- TLS, 610
- Virtual Router Redundancy Protocol (VRRP), 536
- virtual teams in incident response, 991
- virtual tunnel end points (VTEPs), 632
- virtualization
  - backups, 861
  - desktop, 699–701

- virtualized systems
  - containerization, 298–299
  - networks, 704–705
  - overview, 296
  - serverless, 299–301
  - virtual machines, 296–298
  - visual recording devices, 913–916
  - VLAN identifiers (VIDs), 631
  - VLANs (virtual local area networks)
    - latency, 654
    - overview, 630–632
  - VMs. See virtual machines (VMs)
  - VNC (Virtual Network Computing), 700
  - vNICs (virtual NICs), 704–705
  - voice communications, 682
    - cable modems, 686–687
    - DSL, 683–685
    - IP telephony, 687–692
    - ISDN, 685–686
    - PSTN, 682–683
  - voice gateways, 688
  - voice over IP (VoIP) networks
    - business continuity planning, 1069
    - vs. IP telephony, 688
    - overview, 687–688
    - security, 693
    - voice prints, 728
  - voicemail systems, 688
  - voices in information access control, 801

## ▲CISSP All-in-One Exam Guide

- 1318
- voltage in electrical power, 670
- voltage regulators for electric power, 451
- volumetric IDSs, 926
- VPCs (virtual private clouds), 301
- VPNs. See virtual private networks (VPNs)
- VRRP (Virtual Router Redundancy Protocol), 536
- VSATs (very small aperture terminals), 589–590
- VTEPs (virtual tunnel end points), 632
- vulnerabilities
  - defined, 8
  - emergency situations, 869
  - exception handling, 871
  - human, 902–903
  - identifying, 62–63
  - information, 59
  - managing, 900–903
  - overview, 58
  - people, 60
  - processes, 59–60, 902

- remediation, 871
- software, 901, 1133–1134
- testing, 817–822
- vulnerability mapping step in penetration testing, 824
- vulnerability testing vs. penetration tests, 827
- VxLANs (Virtual eXtensible Local Area Networks), 632

## W

- wafer tumbler locks, 919
- waiting room feature for meeting applications, 694
- walkthrough tests in disaster recovery plans, 1063
- walls
  - considerations, 437
  - data processing facilities, 446
- WANs. See wide area networks (WANs)
- WAPs (wireless access points), 564–565
- warded locks, 918
- warez sites, 149–150
- warm sites, 1045–1047
- Wassenaar Arrangement, 145–146
- water and wastewater, 448–450
- water detectors, 445
- water lines, 438
- water sprinklers, 459–460

Waterfall software development, 1095–1096

- watts
  - electrical power, 670–672
  - radio signals, 560
- wave-division multiplexing (WDM), 544
- wave-pattern motion detectors, 927
- WBSs (work breakdown structures) in project management, 1081
- WDM (wave-division multiplexing), 544
- weaponization in Cyber Kill Chain model, 387, 994
- web application security risks, 1134
- web of trust, 367
- web portal functions in FIM systems, 753–754
- web proxies, 665
- web services
  - HTTP, 613–614
  - overview, 611–612
  - REST, 615–616
  - SOAP, 614–615
- Web Services Security (WS-Security or WSS) specification, 615
- well-formed transactions in Clark-Wilson model, 400

- well-known ports, 507
- WEP (Wired Equivalent Privacy), 575–576
- wet chemical fire extinguishers, 459
- wet pipe water sprinkler systems, 460
- whaling, 865
- White, Joe, 20
- white box testing, 826
- whitelisting
  - applications, 225
  - intrusion detection and prevention systems, 968–969
- whole-disk encryption, 255
- Wi-Fi Protected Access 2 (WPA2), 576–578
- wide-angle lenses in CCTV systems, 915
- wide area networks (WANs)
  - ATM, 550–552
  - CSU/DSU, 543–545
  - dedicated links, 541–543
  - frame relay, 547–548
  - HSSI, 552
  - overview, 540
  - switching, 545–547
  - virtual circuits, 548–549
  - X.25, 549–550

## ▲Index

1319

- WIDSs (wireless intrusion detection systems), 967
- WiMAX standard, 569, 587
- windows
  - considerations, 437
  - types, 441
- WIPO (World Intellectual Property Organization), 150
- Wired Equivalent Privacy (WEP), 575–576
- wired windows, 441
- wireless access points (WAPs), 564–565
- wireless intrusion detection systems (WIDSs), 967
- wireless LANs (WLANs)
  - best practices, 582
  - components, 564–565
  - security, 575–582
  - standards, 565–574
- wireless networking
  - chapter questions, 592–595
  - chapter review, 590–592
  - communication techniques overview, 559–561
  - mobile communications, 582–588
  - OFDM, 563–564
  - overview, 559

- satellites, 589–590
- spread spectrum, 561–563
- WLAN components, 564–565
- WLAN security, 575–582
- WLAN standards, 565–574
- wireless personal area networks (WPANs), 570
- wiring closets, 446
- WLANs. See wireless LANs (WLANs)
- Woods, John F., 1079
- work area security, 441–443
- work area separation, 803
- work breakdown structures (WBSs)
  - in project management, 1081
- work factor
  - cryptosystems, 325
  - electrical power, 671
  - work factor in RSA, 342
- work recovery time (WRT) in disaster recovery, 1031–1032
- working images for evidence, 1012
- World Intellectual Property Organization (WIPO), 150
- World Wide Web (WWW), 777

- WPA Enterprise, 577
- WPA2 (Wi-Fi Protected Access 2), 576–578
- WPA3, 578–579
- WPANs (wireless personal area networks), 570
- write-once media for logs, 745, 831
- wrongs against a person category
  - in civil law, 127
- wrongs against property category
  - in civil law, 127
- WRT (work recovery time) in disaster recovery, 1031–1032
- WS-Security specification, 615
- WSS (Web Services Security)
  - specification, 615
- WWW (World Wide Web), 777

## X

- X.25 protocol, 549–550, 552
- X.509 certificates, 359
- XaaS (Everything as a Service), 304–305
- XACML (Extensible Access Control Markup Language), 781
- XDR (extended detection and response)
  - platforms, 968
- XML (Extensible Markup Language), 615, 777
- XOR operation
  - one-time pads, 326–327
  - stream ciphers, 333
- XTACACS (Extended TACACS), 790–791
- YAML Ain't Markup Language (YAML), 615

## Y

Ying, Jun, 20

## Z

Zachman, John, 172, 192

Zachman Framework, 172, 192-194

zero-day attacks, 971

zero knowledge in penetration testing, 825

zero trust principle

network security, 599

secure design, 392

site and facility security, 419-420

third-party connectivity, 706

web services, 612

ZigBee standard, 571-572

Zimmermann, Phil, 367

zombies, 965

## ▲CISSP All-in-One Exam Guide

1320

zone transfers in DNS, 525

zones

access control, 803

CPTED, 429-430

DNS, 525

lighting, 911

Zoom-bombing, 694

zoom in CCTV systems, 914-915

