techniques, and procedures (TTPs).

identification A subject provides some type of data to an authentication service. Identification is the first step in the authentication process.

Identity as a Service (IDaaS) A type of Software as a Service (SaaS) offering that normally provides single sign-on (SSO), federated identity management (IdM), and password management services.

identity management (IdM) A broad term that encompasses the use of different products to identify, authenticate, and authorize users through automated means. It usually includes user account management, access control, credential management, single sign-on (SSO) functionality, managing rights and permissions for user accounts, and auditing and monitoring all of these items.

industrial control system (ICS) Information technology that is specifically designed to control physical devices in industrial processes. The two main types of ICS are distributed control systems (DCSs) and supervisory control and data acquisition (SCADA) systems. The main difference between them is that a DCS controls local processes while SCADA is used to control things remotely.

inference The ability to derive information not explicitly available.

Infrastructure as a Service (IaaS) A cloud computing model that provides users unfettered access to a cloud device, such as an instance of a server, which includes both the operating system and the virtual machine on which it runs.

Integrated Product Team (IPT) A multidisciplinary software development team with representatives from many or all the stakeholder populations.

integrity A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Internet of Things (IoT) The global network of connected, uniquely addressable, embedded systems.

Internet Small Computer System Interface (iSCSI) A converged protocol that encapsulates SCSI data in TCP segments in order to allow peripherals to be connected to computers across networks.

intrusion detection system (IDS) Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms.

intrusion prevention system (IPS) An intrusion detection system (IDS) that is also able to take actions to stop a detected intrusion.

IP Security (IPSec) A suite of protocols that was developed to specifically protect IP traffic. It includes the Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), and Internet Key Exchange (IKE) protocols.

isolation The containment of processes in a system in such a way that they are separated from one another to ensure integrity and confidentiality.

job rotation The practice of ensuring that, over time, more than one person fulfills the tasks of one position within the organization. This enables the organization to have staff backup and redundancy, and helps detect fraudulent activities.

just in time (JIT) access A provisioning methodology that elevates users to the necessary privileged access to perform a specific task.

Kerberos A client/server authentication protocol based on symmetric key cryptography that is the default authentication mechanism in Microsoft Active Directory environments.

kernel The core of an operating system, manages the machine’s hardware resources (including the processor and the memory) and provides and controls the way any other software component accesses these resources.

key A discrete data set that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa, during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as HMACs), which are often used for authentication and integrity.

keystroke monitoring A type of auditing that can review or record keystrokes entered by a user during an active session.

known-plaintext attack A cryptanalysis technique in which the attacker has the plaintext and corresponding ciphertext of one or more messages and wants to discover the key used to encrypt the message(s).

least privilege The secure design principle that requires each subject to be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

⮝Glossary

Li-Fi A wireless networking technology that uses light rather than radio waves to transmit and receive data.

Lightweight Directory Access Protocol (LDAP) A directory service based on a subset of the X.500 standard that allows users and applications to interact with a directory.

link encryption A type of encryption technology that encrypts packets’ headers, trailers, and the data payload. Each network communications node, or hop, must decrypt the packets to read their addresses and routing information and then re-encrypt the packets. This is different from end-to-end encryption.

machine learning (ML) Systems that acquire their knowledge, in the form of numeric parameters (i.e., weights), through training with data sets consisting of millions of examples. In supervised learning, ML systems are told whether or not they made the right decision. In unsupervised training they learn by observing an environment. Finally, in reinforcement learning they get feedback on their decisions from the environment.

maintenance hook Instructions within a program’s code that enable the developer or maintainer to enter the program without having to go through the usual access control and authentication processes. Maintenance hooks should be removed from the code before it is released to production; otherwise, they can cause serious security risks. Also called a back door.

malware Malicious software. Code written to perform activities that circumvent the security policy of a system. Examples are viruses, malicious applets, Trojan horses, logic bombs, and worms.

mandatory access control (MAC) An access policy that restricts subjects’ access to objects based on the security clearance of the subject and the classification of the object. The system enforces the security policy, and users cannot share their files with other users.

message authentication code (MAC) In cryptography, a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message’s integrity (by ensuring that a different MAC will be produced if the message has changed) and its authenticity, because only someone who knows the secret key could have modified the message.

microsegmentation The practice of isolating individual assets (e.g., data servers) in their own protected network environment.

microservice An architectural style that consists of small, decentralized, loosely coupled, individually deployable services built around business capabilities.

multifactor authentication (MFA) Authentication mechanisms that employ more than one factor. Factors are something a person knows (e.g., password), something a person has (e.g., a hardware token), and something a person is (e.g., biometrics).

multilayer protocol

A protocol that works across multiple layers of the OSI model.

multilevel security A class of systems containing information with different classifications. Access decisions are based on the subject’s security clearances, need to know, and formal approval.

Multiprotocol Label Switching (MPLS) A converged data communications protocol designed to improve the routing speed of high-performance networks.

need to know A security principle stating that users should have access only to the information and resources necessary to complete their tasks that fulfill their roles within an organization. Need to know is commonly used in access control criteria by operating systems and applications.

network detection and response (NDR) Systems that monitor network traffic for malicious actors and suspicious behavior, and react and respond to the detection of cyberthreats to the network.

nonrepudiation A service that ensures the sender cannot later falsely deny sending a message or taking an action.

OAuth An open standard for authorization (not authentication) to third parties that lets users authorize a web system to use something that they control at a different website.

object A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains. Examples of objects include records, pages, memory segments, files, directories, directory trees, and programs.

onboarding The process of turning a candidate into a trusted employee who is able to perform all assigned duties.

one-time pad A method of encryption in which the plaintext is combined with a random “pad,” which should be the same length as the plaintext. This encryption process uses a nonrepeating set of random bits that are combined bitwise (XOR) with the message to produce ciphertext. A one-time pad is a perfect encryption scheme because it is unbreakable and each pad is used exactly once, but it is impractical because of all of the required overhead.

Open System Interconnection (OSI) model A conceptual framework used to describe the functions of a networking system along seven layers in which each layer relies on services provided by the layer below it and provides services to the layer above it.

OpenID Connect A simple authentication layer built on top of the OAuth 2.0 protocol that allows transparent authentication and authorization of client resource requests.

password A sequence of characters used to prove one’s identity. It is used during a logon process and should be highly protected.

patent A grant of legal ownership given to an individual or organization to exclude others from using or copying the invention covered by the patent.

Payment Card Industry Data Security Standard (PCI DSS) An information security standard for organizations that are involved in payment card transactions.

penetration testing A method of evaluating the security of a computer system or network by simulating an attack that a malicious hacker would carry out. Pen testing is performed to uncover vulnerabilities and weaknesses.

personnel security The procedures that are established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. Procedures confirm a person’s background and provide assurance of necessary trustworthiness.

physical controls Controls that pertain to controlling individual access into the facility and different departments, locking systems and removing unnecessary USB and optical drives, protecting the perimeter of the facility, monitoring for intrusion, and checking environmental controls.

physical security Controls and procedures put into place to prevent intruders from physically accessing a system or facility. The controls enforce access control and authorized access.

piggyback Unauthorized access to a facility or area by using another user’s legitimate credentials or access rights.

plaintext

In cryptography, the original readable text before it is encrypted.

Platform as a Service (PaaS) A cloud computing model that provides users access to a computing platform but not to the operating system or to the virtual machine on which it runs.

preventive controls

Controls that are intended to keep an incident from occurring.

privacy A security principle that protects an individual’s information and employs controls to ensure that this information is not disseminated or accessed in an unauthorized manner.

privacy by design A secure design principle that ensures privacy of user data is an integral part of the design of an information system, not an afterthought or later-stage feature.

procedure Detailed step-by-step instructions to achieve a certain task, which are used by users, IT staff, operations staff, security members, and others.

protocol A set of rules and formats that enables the standardized exchange of information between different systems.

public key encryption A type of encryption that uses two mathematically related keys to encrypt and decrypt messages. The private key is known only to the owner, and the public key is available to anyone.

public key infrastructure (PKI) A framework of programs, procedures, communication protocols, and public key cryptography that enables a diverse group of individuals to communicate securely.

qualitative risk analysis A risk analysis method that uses opinion and experience to judge an organization’s exposure to risks. It uses scenarios and ratings systems. Compare to quantitative risk analysis.

quantitative risk analysis A risk analysis method that attempts to use percentages in damage estimations and assigns real numbers to the costs of countermeasures for particular risks and the amount of damage that could result from the risk. Compare to qualitative risk analysis.

quantum key distribution (QKD) A system that generates and securely distributes encryption keys of any length between two parties.

RADIUS (Remote Authentication Dial-In User Service) A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism.

recovery point objective (RPO) The acceptable amount of data loss measured in time.

recovery time objective (RTO) The maximum time period within which a missioncritical system must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with a break in business continuity.

reference monitor concept An abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.

registration authority (RA) A trusted entity that establishes and confirms the identity of an individual, initiates the certification process with a CA on behalf of an end user, and performs certificate life-cycle management functions.

reliability The assurance of a given system, or individual component, performing its mission adequately for a specified period of time under the expected operating conditions.

remote journaling A method of transmitting changes to data to an offsite facility. This takes place as parallel processing of transactions, meaning that changes to the data are saved locally and to an offsite facility. These activities take place in real time and provide redundancy and fault tolerance.

repudiation When the sender of a message denies sending the message. The countermeasure to this is to implement digital signatures.

residual risk The remaining risk after the security controls have been applied. The conceptual formulas that explain the difference between total risk and residual risk are

threats × vulnerability × asset value = total risk

(threats × vulnerability × asset value) × controls gap = residual risk

risk The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit a vulnerability.

risk analysis A detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

risk assessment A method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

risk management The process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level of risk.

risk-based access control An authorization mechanism that estimates the risk associated with a particular request in real time and, if it doesn’t exceed a given threshold, grants the subject access to the requested resource.

role-based access control (RBAC) Type of access control model that provides access to resources based on the role the user holds within the organization or the tasks that the user has been assigned.

rule-based access control (RB-RBAC) Type of access control model that uses specific rules that indicate what can and cannot happen between a subject and an object; built on top of traditional RBAC and is thus commonly called RB-RBAC to disambiguate the otherwise overloaded RBAC acronym.

safeguard A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a countermeasure or control.

sandboxing A type of control that isolates processes from the operating system to prevent security violations.

scoping The process of taking a broader standard and trimming out the irrelevant or otherwise unwanted parts.

secure defaults A secure design principle that entails having every system start off in a state where security trumps user friendliness and functionality, and then has controls deliberately relaxed to enable additional features and generally make the system more user friendly.

Security Assertion Markup Language (SAML) An XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

security awareness The knowledge and attitude of an individual concerning likely threats.

security control
security risks.

Any measure taken by an organization to mitigate information

security evaluation Assesses the degree of trust and assurance that can be placed in systems for the secure handling of sensitive information.

security information and event management (SIEM) A software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.

security label

An identifier that represents the security level of an object.

security orchestration, automation, and response (SOAR) Integrated systems that enable more efficient security operations through automation of various workflows.

security testing Testing all security mechanisms and features within a system to determine the level of protection they provide. Security testing can include penetration testing, formal design and implementation verification, and functional testing.

sensitive information Information that would cause a negative effect on the organization if it were lost or compromised.

sensitivity label A piece of information that represents the security level of an object. Sensitivity labels are used as the basis for mandatory access control (MAC) decisions.

separation of duties A secure design principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

serverless architecture A computing architecture in which the services offered to end users, such as compute, storage, or messaging, along with their required configuration and management, can be performed without a requirement from the user to set up any server infrastructure.

service level agreement (SLA) A contract between a service provider and a service user that specifies the minimum acceptable parameters of the services being provided.

shared responsibility A secure design principle that addresses situations in which a service provider is responsible for certain security controls, while the customer is responsible for others.

shoulder surfing When a person looks over another person’s shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.

simple security property A Bell-LaPadula security model rule that stipulates that a subject cannot read data at a higher security level.

single loss expectancy (SLE) A monetary value that is assigned to a single event that represents the organization’s potential loss amount if a specific threat were to take place.

asset value × exposure factor = SLE

single sign-on (SSO) A technology that allows a user to authenticate one time and then access resources in the environment without needing to reauthenticate.

⮝Glossary

social engineering The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

Software as a Service (SaaS) A cloud computing model that provides users access to a specific application that executes in the service provider’s environment.

Software Assurance Maturity Model (SAMM) A maturity model that is specifically focused on secure software development and allows organizations of any size to decide their target maturity levels within each of five critical business functions.

software-defined networking (SDN) An approach to networking that relies on distributed software to provide improved agility and efficiency by centralizing the configuration and control of networking devices.

software-defined security (SDS or SDsec) A security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.

spoofing Presenting false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

standards Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies, applications, parameters, and procedures are carried out in a uniform way across the organization. They are compulsory.

star property (*-property) A Bell-LaPadula security model rule that stipulates that a subject cannot write data to an object at a lower security level.

static application security testing (SAST) A technique, also called static analysis, that identifies certain software defects or security policy violations by examining the source code without executing the program.

subject An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

supervisory control and data acquisition (SCADA) A system for remotely monitoring and controlling physical systems such as power and manufacturing plants.

supply chain An interconnected network of interdependent suppliers and consumers involved in delivering some product or service.

symmetric key cryptography A cryptographic method that uses instances of the same key (called the secret key) for encryption and decryption.

synthetic transaction A transaction that is executed in real time by a software agent to test or monitor the performance of a distributed system.

tabletop exercise (TTX) A type of exercise in which participants respond to notional events to test out procedures and ensure they actually do what they’re intended to and that everyone knows their role in responding to the events.

TACACS (Terminal Access Controller Access Control System) A client/server authentication protocol that provides the same type of functionality as RADIUS and is used as a central access control mechanism mainly for remote users.

tailoring The practice of making changes to specific provisions of a standard so they better address organizational requirements.

technical controls Controls that work in software to provide availability, integrity, or confidentiality protection; also called logical access control mechanisms. Some examples are passwords, identification and authentication methods, security devices, auditing, and the configuration of the network.

test coverage A measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage.

threat A potential cause of an unwanted incident, which can result in harm to a system or organization.

threat intelligence Evidence-based knowledge about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding responses to that menace or hazard.

threat modeling The process of describing probable adverse effects on an organization’s assets caused by specific threat sources.

top-down approach An approach in which the initiation, support, and direction for a project come from top management and work their way down through middle management and then to staff members.

topology The physical construction of how nodes are connected to form a network.

total risk The risk an organization faces if it chooses not to implement any type of safeguard.

trade secret Something that is proprietary to a company and important for its survival and profitability.

trademark A legal right that protects a word, name, product shape, symbol, color, or a combination of these used to identify a product or an organization.

transborder data flow (TDF) The movement of machine-readable data across a political boundary such as a country’s border.

Trojan horse A computer program that has an apparently or actually useful function, but that also contains hidden malicious capabilities to exploit a vulnerability and/or provide unauthorized access into a system.

trust but verify A secure design principle that requires that even when an entity and
its behaviors are trusted, they should be monitored and verified.
user

A person or process that is accessing a computer system.

user and entity behavior analytics (UEBA) Processes that determine normal patterns
of behavior so that abnormalities can be detected and investigated.
user ID
system.

A unique set of characters or code that is used to identify a specific user to a

validation The act of performing tests and evaluations to test a system’s security level
to see if it complies with security specifications and requirements.
Virtual eXtensible Local Area Network (VxLAN) A network virtualization technology
that encapsulates layer 2 frames onto UDP (layer 4) datagrams for distribution anywhere
in the world.
virtualization The practice of running a virtual computing system in an environment
that is abstracted from the actual hardware.
virus A small application, or string of code, that infects applications. The main function
of a virus is to reproduce, and it requires a host application to do this. It can damage data
directly or degrade system performance.
vulnerability A weakness in a system that allows a threat source to compromise its
security. It can be a software, hardware, procedural, or human weakness that can be
exploited.
Waterfall methodology A software development methodology that uses a strictly
linear, sequential life-cycle approach in which each phase must be completed in its
entirety before the next phase can begin.
whitelist (or allow list)
names, or applications.

A set of known-good resources such as IP addresses, domain

work factor The estimated time and effort required for an attacker to overcome a security control.
worm An independent program that can reproduce by copying itself from one system
to another. It may damage data directly or degrade system performance by tying up
resources.
zero trust A secure design principle that assumes that every entity is hostile until
proven otherwise.

⮝This page intentionally left blank

⮝INDEX

A
AARs (after-action reviews) in disaster
recovery, 869, 1061
ABAC (attribute-based access control)
characteristics, 776
description, 774
ABR (available bit rate) in ATM, 551
abstract machines, 766
abstraction
containers, 298
network architectures, 597, 634
object-oriented programming, 1129
programming languages, 1119–1120
system architectures, 283, 297
academic software, 153
acceptable use policies (AUPs)
software, 226
user accounts, 858
web proxies, 664
acceptance risk strategy
ISO/IEC 27005, 178
overview, 79–80
acceptance testing in software
development, 1091
access control
authorization mechanisms.
See authentication; authorization
CPTED, 430–431
facilities, 443–446, 916–924
identity and access, 796
information, 801
just-in-time, 738
locks, 917–923
logical, 717
markup languages, 776–781
models, 766
physical and logical access,
801–803
physical security. See physical
security and controls
remote, 789–795

access control lists (ACLs)
DAC, 767
data historians, 293
identity management, 747
incident response, 996
network sockets, 703
packet-filtering firewalls, 946–948
RBAC, 771

routers, 660
server-based systems, 284
switches, 657
VPNs, 697
WPANs, 571
access doors for data processing facilities, 443
access points (APs)
collision domains, 493
DSL modems, 683
WLANs, 564–565
access triples in Clark-Wilson model, 400
accountability
audits, 741–745
credential management, 736
description, 161, 716
logical access controls, 717
overview, 887–888
Accountability Principle in OECD, 142
accounting in Diameter, 795
accounts
adding, 858
modifying, 859
registration and proofing of identity,
738–740
suspending, 860
accuracy
biometric systems, 724–725, 727
data loss prevention, 270
threat intelligence, 941
ACID properties of database systems, 286
ACK (acknowledgment packets) in TCP
handshakes, 508, 949–951
ACLs. See access control lists (ACLs)
acoustical detection IDSs, 927

acquired software security concerns,
1145–1148
acquiring
data, 230
evidence, 1012–1013
acrylic windows, 441
Act phase in Plan-Do-Check-Act loop, 875
actionability in security metrics, 854
actions in ABAC, 774
actions on objectives stage in Cyber Kill Chain
framework, 994
active attacks on cryptography, 367
Active Directory (AD) environment, 747
active monitors

computer surveillance, 1020
Token Ring, 496
actors
defined, 8
internal, 61–62
ad hoc WLANs, 565
adapters in forensics field kits, 1015
Address Resolution Protocol (ARP), 515–517
Adleman, Leonard, 340
ADM (Architecture Development Method),
194–195
administrative controls
digital asset management, 261
risk responses, 83, 86–87
administrative investigations, 161–162
administrative law system, 128
administrative/regulatory law, 130
administrative responsibilities for locks, 922
admissibility of evidence, 1013–1014
ADSL (asymmetric DSL), 684
Advanced Encryption Standard (AES)
DES replacement, 321
meeting applications, 694
SEDs, 407
TLS, 603–604
WPA2, 578
WPANs, 571
Advanced Micro Devices (AMD)
trade secrets, 149
Advanced Mobile Phone System (AMPS), 584
advanced persistent threats (APTs), 135–136
Advanced Research Project Agency Network
(ARPANET) program, 471
advisory policies, 30

AE (authenticated encryption), 604
AEAD (authenticated encryption with
additional data), 604
AES. See Advanced Encryption Standard (AES)
after-action reviews (AARs) in disaster
recovery, 869, 1061
agent based patch management, 904
agentless patch management, 904
agents
data loss prevention, 273
SNMP, 522–523
aggregation in database systems, 286–287
Agile methodologies
Extreme Programming, 1102
Kanban, 1102–1103
overview, 1100–1101
Scrum, 1101–1102
agreements
disasters recovery, 1047–1048

employment, 36–37
service level. See service level
agreements (SLAs)
AH (Authentication Header) in IPSec, 608
AIKs (attestation identity keys) in Trusted
Platform Modules, 406
alarms
CPTED, 428
doors, 444
duress codes, 931
human-machine interface, 292
perimeter security, 803
ALE (annualized loss expectancy)
control selection, 82
power backup, 448
quantitative risk analysis, 73–75
algorithms
cryptography attacks on, 367–370
cryptology, 320–321
hashing functions, 351–352
patents for, 151
public vs. secret, 369
Align, Plan and Organize (APO) domain in
COBIT 2019, 189
alignment
COBIT goals, 188
security to business strategy,
13–16, 182, 202
strategic, 15–16

🡅Index

allow lists in IDS/IPS, 968–969
alternate category in PACE plans, 1057
always invoked property in reference
monitors, 766
always-on VPN, 697
AMD (Advanced Micro Devices)
trade secrets, 149
amplification DNS attacks, 620
amplitude
analog signals, 644–645
multiplexing systems, 544
radio signals, 559–560
AMPS (Advanced Mobile Phone System), 584
analog transmission, 644–645
analysis
antimalware software, 970
application security, 1139
forensics investigations, 1016–1018
qualitative risk, 72, 76–78
quantitative risk, 72–76, 78–79
software security, 1144–1145

Analysis practice in Good Practice
Guidelines, 106
Android Data company, 150
annualized loss expectancy (ALE)
control selection, 82
power backup, 448
quantitative risk analysis, 73–75
annualized rate of occurrence (ARO), 74–75
annunciator systems in CCTV systems, 916
anomalies, session termination from, 741
anomaly-based IDS/IPS, 967–968
antimalware software, 969–972
anycast addresses in IPv6, 513
APIs. See application programming
interfaces (APIs)
APO (Align, Plan and Organize) domain
in COBIT 2019, 189
apparent power, 671
appendices in reports, 873
Apple lawsuit, 151
appliances, 958
application errors in risk management, 54
application layer
functions and protocols, 483
OSI model, 474–475
application-level events in audits, 743
application-level proxies, 953–955, 957

application programming interfaces (APIs)
application layer, 475
CASBs, 275–276
containers, 298
description, 837
object-oriented programming, 1126–1128
SDNs, 635
software libraries, 1132–1133
software security, 1132
TEE, 409
web services, 613
applications
access control, 802
connections, 479
security testing, 1139–1140
whitelisting, 225
approval by management, 877
APs (access points)
collision domains, 493
DSL modems, 683
WLANs, 564–565
APT32, 389
APTs (advanced persistent threats), 135–136
architects for software development, 1080
Architecture Development Method (ADM),
194–195

architectures. See system architectures
archive bits for backups, 1035
archives for data, 239–240
Arnold, Benedict, 319
ARO (annualized rate of occurrence), 74–75
ARP (Address Resolution Protocol), 515–517
ARPANET (Advanced Research Project
Agency Network) program, 471
artifacts in digital forensics, 1020–1021
ASOR (authoritative system of record), 739
ASs (autonomous systems), 533
assemblers, 1118, 1120–1122
assembly language, 1118, 1120
assessments
audits, 838–844
chapter questions, 846–849
chapter review, 844–846
designing, 814–815
disaster recovery plans, 1058
overview, 813
physical security, 908
preventive and detective measures, 945

assessments (cont.)
risk. See risk assessment
Risk Management Framework, 176
social engineering, 903
software security, 1144–1148
strategies, 813–816
technical controls. See testing
validating, 815–816
assets
business impact analysis, 112–115
chapter questions, 247–251
chapter review, 245–246
classification, 219
data life cycle. See data life cycle
digital, 258–259, 261–263
information, 214–219
inventories, 224–227
life cycle, 222–230
overview, 213–214
ownership, 223
physical security, 220–222
provisioning, 227–228
retention, 228–230
valuation, 65–66
assisted password resets, 738
associations in misuse case testing, 835
ASTM International fire resistance
ratings, 456

asymmetric DSL (ADSL), 684
asymmetric key cryptography, 328
Diffie-Hellman algorithm,
337–340
overview, 335–337
RSA, 340–342
summary, 337
with symmetric, 346–349
asynchronous replication, 1039
asynchronous token devices for one-time
passwords, 731
Asynchronous Transfer Mode (ATM) in
WANs, 550–552
asynchronous transmissions, 645–647
atbash cryptology, 317–318
ATM (Asynchronous Transfer Mode)
in WANs, 550–552
atomic execution in trusted execution
environments, 410
atomicity in ACID properties, 286

attack surface analysis in software
development design, 1085
attack trees in threat modeling, 386–387
attacks, evolution of, 134–138
attenuation in cabling, 652
attestation identity keys (AIKs) in Trusted
Platform Modules, 406
attocells in Li-Fi standard, 568
attribute-based access control (ABAC)
characteristics, 776
description, 774
attribute-value pairs (AVPs) in RADIUS, 792
attributes
LDAP, 749
object-oriented programming, 1125
audience for reports, 872
audit-reduction tools, 744
auditors, 25
audits
accountability, 741–742
application-level events, 743
external, 842–843
internal, 840–842
overview, 838–840
physical security, 929
protecting, 744–745
reviewing, 743–744
software security, 1147
strategies, 813–816
system-level events, 742
third-party, 843–844
user-level events:, 743
AUPs (acceptable use policies)

software, 226
user accounts, 858
web proxies, 664
authenticated encryption (AE), 604
authenticated encryption with additional
data (AEAD), 604
authentication. See also authorization
access control and markup languages,
776–781
asymmetric key cryptography, 336
biometric. See biometric authentication
cryptosystems, 323
description, 716
Diameter, 794–795
802.11, 580

⬆Index

factors, 718–719
Internet of Things, 306
Kerberos, 785–788
knowledge-based, 720–723
network sockets, 703
ownership-based, 729–734
quorum, 34
race conditions, 717
VPNs, 697–699
Authentication Header (AH) in IPSec, 608
authenticators in Kerberos, 786–787
authenticity, 6
authoritative name servers in DNS, 525
authoritative system of record (ASOR), 739
authority
disaster recovery goals, 1054
URLs, 613
authorization. See also authentication
ABAC, 774
access control and markup languages,
776–781
cryptosystems, 324
DAC, 766–768
data loss prevention, 267, 271
description, 716
Diameter, 795
e-mail, 624
IP telephony, 692
Kerberos, 784–789
MAC, 768–771
OAuth, 782–783
OpenID Connect, 783–784
overview, 765–766
race conditions, 717
RB-RBAC, 774

risk-based access control, 775–776
Risk Management Framework, 176
role-based access control, 771–773
authorization code flow in OIDC, 784
authorization creep
description, 395
privileged accounts, 889
role changes, 799
user accounts, 859
authorization servers in OAuth, 782
auto iris lenses in CCTV systems, 915
automated risk analysis methods, 73
automated scanning of devices, 226

automated tests in software
development, 1091
automatic tunneling in IPv6, 514
automation
backups, 863
configuration management, 895
HMIs, 292
SOAR, 980
virtualization, 861
ZigBee, 571
autonomous systems (ASs), 533
availability
business continuity, 103
business continuity planning, 1067–1070
CIA triad, 7–8
disaster recovery, 1049–1053
fault tolerance and system resilience, 1051
high, 1050–1053
overview, 6
quality of service, 1050–1051
available bit rate (ABR) in ATM, 551
avalanche effect in symmetric key
cryptography, 332
avoidance risk strategy
ISO/IEC 27005, 178
overview, 79
AVPs (attribute-value pairs) in RADIUS, 792
awareness programs
content reviews, 43
culture factors, 867
data protection, 867
disaster recovery plans, 1060–1061
effectiveness evaluation, 43–44
employees, 266
goals, 40
methods and techniques, 40–44
online safety, 866–867
overview, 863–864
personnel, 930–931
social engineering, 864–866

AXELOS, 196

B
B channels in ISDN, 686
B2B (business-to-business) transactions in SAML, 780
B2C (business-to-consumer) transactions in SAML, 780

back doors in software development, 1091
back-off algorithm in CSMA, 491
background checks in candidate screening and hiring, 35–36
background elements in reports, 873
backup administrators, 1035
backup lighting, 912
backups
vs. archives, 239–240
business continuity planning, 1069–1070
data loss prevention, 269
digital asset management, 261–262
electric power, 448–450, 671
facilities, 1040–1041
hierarchical storage management, 898–899
overview, 1034–1037
protecting, 896–899
restoring, 1037, 1041–1042
strategies, 1037–1040
verification, 860–862
BAI (Build, Acquire and Implement) domain in COBIT 2019, 189
balanced security, 7–8
bandwidth
ATM, 550
cable modems, 686–687
cabling, 654–655
coaxial cable, 649
dedicated links, 541–542
distribution facilities, 446
DSL, 683–684
frame relay, 547–548
ISDN, 685–686
optical carriers, 543
proxy servers, 664
PVCs, 549
QoS, 551–552, 1050
satellite communications, 588
server-based systems, 300
switches, 658
unmanaged patching threat, 904
VoIP, 688

WANs, 543
barriers in physical security, 908
BAS (breach and attack simulations), 828
baseband transmission, 647–648
Baseline Privacy Interface/Security (BPI/SEC)
specifications, 687

baselines, 31–32
anomaly-based IDS/IPS, 968
configuration management, 894
ISO/IEC 27004, 852
Basic CIS controls, 187
Basic Rate Interface (BRI) ISDN, 685–686
bastion hosts, 965
BC. See business continuity (BC)
BCM (business continuity management),
102–105
enterprise security program, 106–108
Professional Practices for Business
Continuity Management, 106
BCP. See business continuity planning (BCP)
beaconing in Token Ring, 496
beamforming, 567
behavior blocking in antimalware software,
970–971
behavioral biometric authentication, 724
behavioral model for software development
design, 1084
Bell, Alexander Graham, 681
Bell-LaPadula model, 398–399, 403
benches, 431
Berners-Lee, Tim, 253
best-effort protocols, 503
best-effort service in QoS, 551
best practices in business continuity, 104–106
BGP (Border Gateway Protocol), 536–537
BIA. See business impact analysis (BIA)
Biba model, 399–400, 403
big data, retaining, 235
biometric authentication, 727
facial scans, 728
fingerprints, 726
hand geometry, 727
hand topography, 728–729
iris scans, 727
issues and concerns, 729
keystroke dynamics, 728
overview, 723–726
retina scans, 727
signature dynamics, 727–728
voice prints, 728
birthday attacks, 353–354
BISDN (Broadband ISDN), 685
bitcoin, 307

BitTorrent protocol, 149, 307

🡅Index

black box testing, 826
black holes, 535, 975
blacklisting in IDS/IPS, 968–969
blackouts, 451
blind penetration testing, 825–826
block ciphers, 330–333
Bluejacking, 573
blueprints in frameworks, 201–203
Bluesnarfing, 573
Bluetooth wireless technology, 572–573
board members, risk reporting for, 94–95
bollards, 429, 910–911
BOOTP (Bootstrap Protocol), 519
Border Gateway Protocol (BGP), 536–537
botnets, 134
bots, 134
boundary conditions in interface testing, 837
BPC (business process compromise) attacks, 59–60
BPI/SEC (Baseline Privacy Interface/Security) specifications, 687
branches in tabletop exercises, 1063
brand issues in disaster recovery, 1054
BrandScope attacks, 257
Brazil, General Personal Data Protection Law in, 144
breach and attack simulations (BAS), 828
breaches. See data breaches
Brewer and Nash model, 402–403
BRI (Basic Rate Interface) ISDN, 685–686
bridges
characteristics, 665
forwarding tables, 656–657
overview, 656
vs. routers, 657
bring your own devices (BYOD), 220
Broadband ISDN (BISDN), 685
broadband transmission vs. baseband, 647–648
broadband wireless access, 569
broadcast domains in medium access control, 492–494
broadcast storms in bridges, 656
broadcast transmission in local area networks, 499–500
Broken Windows, 433

brownouts, 451
brute-force attacks
cryptography, 325, 368
passwords, 721
BSA (Business Software Alliance),
154, 226
Budapest Convention, 139
buffer overflows
description, 819
software development, 1089–1090
buffers, emulation, 970
Build, Acquire and Implement (BAI) domain
in COBIT 2019, 189
building codes, 436–437
bulletproof doors, 440
bump keys, 924
bus encryption, 407–408
bus topology, 487–488
business continuity (BC)
BCP life cycle, 1065–1067
business impact analysis, 108–115
description, 1030
enterprise security program, 106–108
overview, 101–104, 867–869, 1065
standards and best practices, 104–106
Business Continuity Institute, Good Practice
Guidelines, 105–106
business continuity management (BCM),
102–105
enterprise security program, 106–108
Professional Practices for Business
Continuity Management, 106
business continuity planning (BCP),
101–105
end-user environment, 1071
enterprise security program, 108
hardware backups, 1069–1070
information systems availability,
1067–1070
life cycle, 1065–1067
overview, 107, 1065
storing, 1042
teams, 1030
business critical data in disaster
recovery, 1032
business enablement, 16
business entry rule in evidence
admissibility, 1014

business impact analysis (BIA), 104–105
asset value, 112–115

disaster recovery, 1032
overview, 108–109
risk assessment, 109–112
steps, 112
business process compromise (BPC) attacks, 59–60
business process recovery, 1033–1034
Business Software Alliance (BSA), 154, 226
business strategy, aligning security to, 13–16
business-to-business (B2B) transactions in SAML, 780
business-to-consumer (B2C) transactions in SAML, 780
business unit leads on incident response teams, 1001
business units in incident notifications, 1004
BYE messages in SIP, 689–690
BYOD (bring your own devices), 220
bytecode in Java programming language, 1122–1123

C
C programming language, 1121–1122
cable modems, 686–687
cable traps, 921
cabling
bandwidth and throughput, 654–655
coaxial cable, 649
fiber-optic cable, 650–651
forensics field kits, 1015
overview, 648
problems, 651–653
twisted-pair cabling, 649–650
CABs (change advisory boards)
policies for, 891
purpose, 93
software development tools, 1138
cache poisoning, ARP table, 516–517
Caesar, Julius, 318
Caesar cipher, 318–319
California Consumer Privacy Act (CCPA), 141–142
call-processing managers, 688
call trees in disaster recovery plans, 1056
cameras in CCTV systems, 916
CAN (Controller Area Network) bus, 627

Canada, Personal Information Protection and Electronic Documents Act in, 147
Capability Maturity Model (CMM), 197–199
Capability Maturity Model Integration (CMMI), 1107–1109
capacitance detectors, 927

CAPTCHA data, 723
card badge readers, 925
care-of addresses in mobile IP, 793
carrier sense multiple access (CSMA), 490–491
carrier sense multiple access with collision avoidance (CSMA/CA), 491
carrier sense multiple access with collision detection (CSMA/CD), 491
carriers in steganography, 265
CART acronym in threat intelligence, 941
CAs (certificate authorities), 360–362
CASBs (cloud access security brokers), 275–276
cascading errors, 62
CASE (computer-aided software engineering) tools, 1087
catastrophes, 1043
categorize step in Risk Management Framework, 174–175
CBC-MAC (CCM), 578
CBEST standard, 156
CBKE (Certificate-Based Key Establishment) protocol, 572
CBR (constant bit rate) in ATM, 551
CCDs (charged-coupled devices), 914
CCM (CBC-MAC), 578
CCPA (California Consumer Privacy Act), 141–142
CCTV (closed-circuit TV) systems, 913–916
CD (continuous delivery) in software security, 1140–1141
CDDI (Copper Distributed Data Interface), 497
CDIs (constrained data items) in Clark-Wilson model, 400
CDMA (code division multiple access), 584–585
CDNs (content distribution networks), 308, 674

🡅Index

ceilings
considerations, 437
dropped, 442
RFI issues, 450
cell suppression in database systems, 288
Center for Internet Security (CIS) framework
CIS Controls Measures and Metrics document, 92
security controls, 172, 185–187

centralized patch management, 904–905
Centripetal Networks, 151
CEOs (chief executive officers), 19–21
CER (crossover error rate) in biometric
authentication, 724–725
CERT (Computer Emergency Response
Team), 993
CERT Advisory for privacy issues, 1014
CERT/CC (Computer Emergency Response
Team Coordination Center), 901
certificate authorities (CAs), 360–362
Certificate-Based Key Establishment (CBKE)
protocol, 572
certificate revocation lists (CRLs), 361–362
certificates in PKI, 359–360
certifications, 40–41
CFOs (chief financial officers), 19–20
chain of custody for evidence, 1010–1011
Challenge Handshake Authentication
Protocol (CHAP), 698
change
data loss prevention for, 270
digital asset management, 262
monitoring, 92–93
change advisory boards (CABs)
policies for, 891
purpose, 93
software development tools, 1138
change control analysts, 24
change management, 891
vs. configuration management, 895
documentation, 893
practices, 891–892
runbooks, 1006
software development, 1092–1094
software security, 1145
change management boards, 223
channel service unit/data service
unit (CSU/DSU), 543–545

channels
access points, 565
for attacks, 474
CHAP (Challenge Handshake Authentication
Protocol), 698
charged-coupled devices (CCDs), 914
Check phase in Plan-Do-Check-Act
loop, 875
checkers, password, 722
checklist tests in disaster recovery plans,
1062–1063
chemical fire extinguishers, 459
chests for data protection, 222
Cheyenne Mountain complex, 436

chief executive officers (CEOs), 19–21
chief financial officers (CFOs), 19–20
chief human resources officers (CHROs), 990
chief information officers (CIOs),
19–21, 990
chief information security officers (CISOs)
IMPs, 990
incident notifications, 1004
incident response teams, 1001
role, 22
chief operations officers (COOs), 990
chief privacy officers (CPOs), 21
chief security officers (CSOs), 22
Chinese Remainder
Theorem (RSA-CRT), 372
Chinese Wall model, 402–403
chipping code in DSSS, 562
chips in DSSS, 562
chosen-ciphertext attacks, 369
chosen-plaintext attacks, 368–369
CHROs (chief human resources officers), 990
CI (continuous integration) in software
security, 1140–1141
CIA triad, 7–8
CIDR (classless interdomain routing), 512
CIOs (chief information officers), 19–21, 990
cipher locks, 920–921
ciphers in cryptology, 318–321
ciphertext-only attacks, 368
CIR (committed information rate) in frame
relay, 547–548
circuit-level proxies, 953–957
circuit switching in WANs, 545–547
circumventing locks, 922–924

CIS (Center for Internet Security) framework
CIS Controls Measures and Metrics
document, 92
security controls, 172, 185–187
Cisco Systems, 151
CISOs. See chief information security
officers (CISOs)
civil investigations, 162
civil law, 126–129
Clark-Wilson model, 400, 403
classes
IP addresses, 510
object-oriented programming, 1125–1127
classification
artificial intelligence tools, 977
data retention, 236

incidents, 1002–1003
information, 215–219
classless interdomain routing (CIDR), 512
classless IP addresses, 512
clean desk policy, 442–443
cleanroom methodology in software
development, 1105
clearing media, 259
client-based systems, 284
client/server systems, 284
clipping levels for failed logon attempts, 721
close stage in change management, 892
CLOSE-WAIT state in TCP connections, 951
closed-circuit TV (CCTV) systems, 913–916
CLOSING state in TCP connections, 951
cloud access security brokers (CASBs), 275–276
cloud-based systems
asset provisioning, 228
backups, 1038
deployment models, 305
FIM systems, 756
frame relay, 548
IaaS, 304
overview, 301–302
PaaS, 302–304
SaaS, 302–303
XaaS, 304–305
clustered servers in quality of service, 1051
clustering for artificial intelligence tools, 978
CM. See configuration management (CM)
CMDB (configuration management
database), 895

CMF (collection management framework)
forensics investigations, 1016–1017
logs, 978
threat intelligence, 942
CMM (Capability Maturity Model), 197–199
CMMI (Capability Maturity Model
Integration), 1107–1109
CO2 fire suppression, 458
coaxial cable, 649
COBIT 2019 framework, 172, 187–189
code and coding
bloat, 833
obfuscation, 905
repositories, 1143–1144
reviews, 833–834
secure practices, 1134–1136
testing, 834–835
code division multiple access (CDMA),
584–585
code law, 126
Code of Ethics, 44–45

Codecov platform, 1141
CoE (Council of Europe), 139
cognitive passwords, 723
cohesion in software, 1130–1132
COI (community of interest) as threat data
source, 943
cold sites in disaster recovery, 1045–1047
collection
data, 231–232
evidence, 1010–1012
Collection Limitation Principle in OECD, 142
collection management framework (CMF)
forensics investigations, 1016–1017
logs, 978
threat intelligence, 942
collision free hashing algorithms, 351–352
collisions
CSMA, 490
hashing functions, 353
medium access control, 492–494
collusion, 34
COM domain in DNS, 527
combi smart cards, 734
combination locks, 920
Command and Control
Cyber Kill Chain model, 388, 994
MITRE ATT&CK framework, 389

↑Index

commercial off-the-shelf (COTS) software
description, 153
security concerns, 1146
committed information rate (CIR) in frame
relay, 547–548
common controls in Risk Management
Framework, 175
common law, 126–130
Common Weakness Enumeration (CWE)
initiative, 1088
communication
audit results, 839–840
in disaster recovery plans, 1056–1057
employees, 266
object-oriented programming, 1126
communications channels
chapter questions, 709–712
chapter review, 707–709
data, 702–704
multimedia collaboration, 693–696
overview, 681
remote access, 696–702
third-party connectivity, 705–706

virtualized networks, 704–705
voice. See voice communications
community clouds, 305
community of interest (COI) as threat data source, 943
community strings in SNMP, 522–524
comparability of security metrics, 854–855
compartmentalizing information in forensics investigation interviews, 1019
compensating controls in risk responses, 85, 87–88
compiled code, software escrow for, 1143
compilers, 1119–1122
complete characteristic of threat intelligence, 941
complexities in cybercrimes, 132–134
compliance
audits, 844
chapter questions, 165–169
chapter review, 162–165
checks, 838
cybercrimes, 130–139
data breaches, 139–147
identity and access, 796–797
investigation requirements, 161–162

laws and regulations, 125–130
liability and ramifications, 158–161
licensing and intellectual property requirements, 147–154
monitoring, 93–94
overview, 125
policies, 39–40
requirements, 155–161
compromise assessments, 17
computer-aided software engineering (CASE) tools, 1087
computer-assisted crimes, 130–131
Computer Emergency Response Team (CERT), 993
Computer Emergency Response Team Coordination Center (CERT/CC), 901
Computer Ethics Institute, 45–46
“computer is incidental” crimes, 130–131
computer surveillance, 1020
computer system connections, 479
computer-targeted crimes, 130–131
concentrators, 655
concurrency management in software, 1142
conference call bridges in H.323, 689
confidential classification level, 216–217
confidentiality
asymmetric key cryptography, 336
audit logs, 745

Bell-LaPadula model, 398
business continuity, 102–103
CIA triad, 8, 64
cryptosystems, 323–324, 330
customer relations, 174–175
DNS over HTTPS, 621
forensics investigation interviews, 1019
overview, 4–5
TLS, 602
VPNs, 605
configuration management (CM)
automation, 895
baselining, 894
vs. change management, 895
identity and access, 799
overview, 893–894
preventive and detective measures, 944
provisioning, 894–895
secure software, 1142
unmanaged patching threat, 904

configuration management database
(CMDB), 895
confusion in symmetric key cryptography, 331
congestion
TCP vs. UDP, 503, 506
throughput, 654
connection-oriented protocols
description, 479
TCP, 503–504
connectionless protocols
description, 479
UDP, 503–504
connections in TCP vs. UDP, 506
connectivity for federated identity, 754–755
consent provision in GDPR, 144–145
consistency in ACID properties, 286
constant bit rate (CBR) in ATM, 551
constrained data items (CDIs) in ClarkWilson model, 400
construction issues, 436–439
consultants, 39
consumer-grade products for meeting
applications, 694
contact smart cards, 733
contactless smart cards, 733–734
containerization, 298–299
content-dependent access control in database
systems, 287
content distribution networks (CDNs),
308, 674
content reviews, periodic, 43

context-dependent access control for database systems, 287–288
context in ABAC, 774
contingency category in PACE plans, 1057
contingency strategies in business continuity, 104–105
contingency suppliers in disaster recovery, 1046
continuous delivery (CD) in software security, 1140–1141
continuous improvement in risk management, 95–96
continuous integration (CI) in software security, 1140–1141
continuous lighting, 912
continuous monitoring, 981–982
contractors, 39
contractual requirements compliance, 156–158

control planes in SDNs, 633–634
control zones, 803
controlled unclassified data, 216–217
Controller Area Network (CAN) bus, 627
controllers, data, 244
controls
assessments. See testing
CPTED, 430–431
data states, 254–258
defined, 9
digital asset management, 261–262
frameworks, 172, 183–189
overview, 253–254
preventive and detective measures, 944
scoping and tailoring, 258
standards, 258
threat modeling, 387
controls for risk response
assessments, 88–91
selection, 82–83
types, 83–88
controls for secure software
application testing, 1139–1140
code repositories, 1143–1144
continuous integration and delivery, 1140–1141
development platforms, 1137–1138
overview, 1136–1137
SOAR, 1141–1142
software configuration management, 1142
tool sets, 1138
controls for site and facilities
data processing facilities, 443–446
distribution facilities, 446–447
environmental issues, 461
fire safety, 454–460

storage facilities, 447–448
utilities, 448–454
work area security, 441–443
Convention on Cybercrime, 139
converged protocols, 627–628
cookies for web services, 613
coordinators in WPANs, 570
COOs (chief operations officers), 990
copper cable, 649–650
Copper Distributed Data
Interface (CDDI), 497
Copyright Directive, 155

copyrights, 149–150
core RBAC, 772
corrective controls in risk response, 85, 87
cost approach in executive summaries, 874
cost/benefit comparisons in risk assessment,
64, 82
costs
outsourced security services, 974
smart cards, 734
COTS (commercial off-the-shelf) software
description, 153
security concerns, 1146
Council of Europe (CoE), 139
Counter Mode Cipher Block Chaining
Message Authentication Code Protocol, 578
countermeasures
defined, 9
risk responses, 81–83
coupling in software, 1130–1132
coverage for backups, 863
covert channels, 401
covert timing channels, 401
CPOs (chief privacy officers), 21
CPTED. See Crime Prevention Through
Environmental Design (CPTED)
crackers for passwords, 722
create, read, update, and delete (CRUD)
actions for database systems, 285–287
credential management
accountability, 741–745
just-in-time access, 738
overview, 736
password managers, 736–737
password resets, 737–738
password synchronization, 737
profile updates, 740
registration and proofing of identity,
738–740

session management, 740–741
unmanaged patching threat, 904
Crime Prevention Through Environmental
Design (CPTED)
landscaping, 908
maintenance, 433
natural access control, 428–431
natural surveillance, 431
overview, 427–428
territorial reinforcement, 431–432

crimes. See also incidents
crime scene control, 1010
detection goals, 424
evidence collection and handling, 1008
incident investigations, 1006–1008
incident response, 992
investigation requirements, 162
criminal law system, 127, 129
critical data backups, 1037
criticality of data, 215
criticality values in disaster recovery, 1032
CRLs (certificate revocation lists),
361–362
cross-certification, 361
cross-sectional photoelectric cells, 927
crossover error rate (CER) in biometric
authentication, 724–725
crosstalk in cabling, 653
CRUD (create, read, update, and delete)
actions for database systems, 285–287
cryptanalysis, 317
cryptographic hash chaining, 831
cryptology. See also encryption
asymmetric key, 335–342
attacks against, 367–375
chapter questions, 379–383
chapter review, 375–378
cryptosystems, 323–325
definitions and concepts, 321–323
ECC, 342–343
hardware vs. software systems, 602
history, 317–321
hybrid encryption methods, 346–350
integrity, 351–358
IP telephony, 692
Kerckhoffs’ Principle, 324–325
life cycle, 328
methods overview, 328
one-time pads, 325–328
overview, 317
PKI, 359–367
quantum, 344–346
symmetric key, 329–335

cryptoprocessors for bus encryption, 408
cryptosystems
components, 323–324
description, 321
strength, 325

cryptovariables, 322
CSMA (carrier sense multiple access), 490–491
CSMA/CA (carrier sense multiple access with collision avoidance), 491
CSMA/CD (carrier sense multiple access with collision detection), 491
CSOs (chief security officers), 22
CSU/DSU (channel service unit/data service unit), 543–545
culture
data prevention strategies, 269
DevOps, 1104
employee matches, 35
internal audits, 841
risk analysis teams, 76, 78
security awareness, 867
current in electrical power, 670
custodians, data, 244
customary law system, 128
customers
confidentiality for, 174–175
incident notifications to, 1004
CWE (Common Weakness Enumeration) initiative, 1088
Cyber Kill Chain framework, 387–389, 994–995
cyber-physical systems, 306
cybercrimes and data breaches
common schemes, 137
complexities, 132–134
evolution of attacks, 134–138
international issues, 138–139
overview, 130–132
cybercriminals, 60
cybersecurity analysts
incident response teams, 1001
tasks and responsibilities, 886
Cybersecurity Framework, 172, 182
cybersecurity governance
aligning security to business strategy, 13–16
authenticity, 6
availability, 6
balanced security, 7–8
baselines, 31–32

chapter questions, 48–52
chapter review, 46–48
concepts and terms, 4–10

confidentiality, 5
education and training, 40–44
guidelines, 32
implementation, 32–33
integrity, 5–6
miscellaneous terms, 8–10
nonrepudiation, 6–7
organizational processes, 17–18
organizational roles and responsibilities, 18–25
overview, 3–4
personnel security, 33–40
principles, 10–12
procedures, 32
professional ethics, 44–46
security overview, 25–27
security policies, 27–29
standards, 29–31
cyberthreat hunting, 943

D
D-AMPS (Digital AMPS), 584
D channels in ISDN, 686
DAC (discretionary access control)
challenges, 768
characteristics, 776
overview, 766–767
DACs (dual-attached concentrators) in FDDI, 498
damage assessment in disaster recovery plans, 1058
DASs (data acquisition servers) in SCADA systems, 294
DASs (dual-attachment stations) in FDDI, 498
DAST (dynamic application security testing), 1139
data
acquisition, 230
archival, 239–240
backups, 861–862, 1034–1041
classification, 215–216
collection, 231–232
destruction, 240–244
roles, 244–245
sharing, 238–239
storage, 232–233
use, 237–238

🡅Index

1267
data acquisition servers (DASs) in SCADA systems, 294
data analysts, 24
data at rest
description, 59
overview, 254–255
data breaches
Codecov, 1141
European Union Laws, 142–144
GDPR, 144
import/export controls, 145–146
overview, 139–141
PII, 140–141
privacy, 147
transborder data flow, 146–147
U.S. laws, 141–142
data communications, 702
application layer, 474–475
data link layer, 480–483
functions and protocols, 483–485
layers together, 485–487
network layer, 480
network reference models, 470–471
network sockets, 703
overview, 469–470
physical layer, 483
presentation layer, 475–476
protocols, 471–474
remote procedure calls, 703–704
session layer, 477–478
transport layer, 479–480
data controllers in GDPR, 143
data custodians, 23
data diodes, 293, 831
Data Encryption Standard (DES), 321
data flows in data loss prevention, 268–269
data hiding in object-oriented programming, 1128
data historians, 293
data in motion/transit
description, 59
overview, 254–256
data in use
description, 59
overview, 254, 256–258

data leaks, 267
data life cycle
data acquisition, 230

data archival, 239–240
data collection, 231–232
data destruction, 240–244
data loss prevention, 269
data retention, 233–236
data roles, 244–245
data sharing, 238–239
data storage, 232–233
data use, 237–238
e-discovery, 236–237
overview, 230
data link layer
functions and protocols, 484–485
OSI model, 480–483
protocols, 646
data localization laws, 146–147, 232
data loss prevention (DLP)
approaches, 267
awareness programs, 867
data flows, 268–269
endpoint, 273–274
hybrid, 274
inventories, 267–268
network, 272–273
overview, 265–267
protection strategies, 269–271
SOAR, 1142
Data-Over-Cable Service Interface
Specifications (DOCSIS), 687
data owners, 22–23
data processing facilities, 443–446
data processors in GDPR, 143
Data Protection Directive (DPD), 143
data protection methods
cloud access security brokers, 275–276
data loss prevention, 265–274
digital asset management, 261–263
Digital Rights Management, 263–265
overview, 258–261
Data Protection Officers (DPOs)
in GDPR, 144
Data Quality Principle in OECD, 142
data retention
overview, 233
policies, 234–236

data security
chapter questions, 277–279
chapter review, 276–277
controls, 253–258
overview, 253

protection methods. See data protection methods
supply chain risk management, 100
data sovereignty laws, 232
data states in controls, 254–258
data structures in TCP, 509
data subjects in GDPR, 143
database management systems (DBMSs), 285–286
database systems, 285
ACID properties, 286
backups, 861
directory services, 747
securing, 286–288
dating evidence, 1010
DBMSs (database management systems), 285–286
DCs (domain controllers) in directory services, 747–748
DCSs (distributed control systems), 290, 293
DDoS (distributed denial-of-service) attacks
CDNs for, 674
DNS, 619–620
PaaS for, 303
DDR (dial-on-demand routing), 686
decision stage in forensics investigations, 1016–1017
decommissioning assets, 229–230
dedicated lines for WANs, 541–543, 552
defaults
network, 598
secure, 396–397, 422
third-party connectivity, 706
web services, 611
defects per KLOC, 395
defense in depth
controls for, 84
design principle, 390–392
HTTPS, 614
network security, 598
physical security, 906
site and facility security, 419
third-party connectivity, 706

deferred commitment in object-oriented programming, 1127
defined level in CMMI, 1108
degaussing media, 243, 261
degrees, 40–41
delay time for locks, 918, 920
delayed loss risk, 63
delaying mechanisms in site planning, 424
Deliver, Service and Support (DSS) domain

in COBIT 2019, 189
delivery stage in Cyber Kill Chain model,
388, 994
Delphi technique, 77
deluge water sprinkler systems, 460
DeMarco, Tom, 283
demilitarized zones (DMZs) for firewalls
dual-homed, 959
functions, 945–946
screened subnet, 960
denial-of-service (DoS) attacks
STRIDE model, 388
wireless communications, 578
Denis Trojan, 389
deny lists in IDS/IPS, 968–969
Department of Defense Architecture
Framework (DoDAF), 173, 195
depositories, protecting, 222
deprovisioning accounts, 800
depth of field in CCTV systems, 915
DES (Data Encryption Standard), 321
design
assessments, 814–815
network security, 597–599
SDLC, 1080, 1083–1087
secure. See secure design principles
site and facility security, 417–418
software. See secure software; software
development
Design function in SAMM, 1109
Design practice in Good Practice
Guidelines, 106
desktop virtualization, 699–701
destroying data, 240–244
detection
fire safety, 454–457
Framework Core, 182
incidents, 995–996

detective controls in risk responses, 85, 87
deterrent controls in risk responses, 85, 87
deterrents in physical security, 908
development platforms for software,
1137–1138
development stage in SDLC,
1080, 1087–1089
device locks, 922–923
devices
access control, 802
industrial control systems, 291–293
IP telephony, 688

management software, 226
DevOps, 1103–1104
DevSecOps
software development, 1104
software security, 1144–1145
DFS (Dynamic Frequency Selection), 574
DGAs (domain generation algorithms) in
DNS, 617–618
DHCP (Dynamic Host Configuration
Protocol)
IP addresses, 501
overview, 517–519
DHCPACK packets, 518–519
DHCPDISCOVER packets, 518–519
DHCPOFFER packets, 518–519
DHCPREQUEST packets, 518–519
diagonal filters in QKD, 344
diagrams, network, 668–670
dial-on-demand routing (DDR), 686
dial-up connections, 684
dialog management, 477
Diameter protocol, 793–795
dictionary attacks on passwords, 721
differential backups, 1035–1036
differential cryptanalysis attacks,
369–370
differential power analysis for smart
cards, 735
differentiated service in QoS, 551
Diffie, Whitfield, 337–340
Diffie-Hellman algorithm, 337–340
diffusion in symmetric key cryptography,
331–332
digital acquisition of evidence, 1012
Digital AMPS (D-AMPS), 584
digital certificates in PKI, 359–360

digital forensics
artifacts, 1020–1021
field kits, 1015
interviews, 1018–1019
investigation techniques, 1016–1018
overview, 1015–1016
reporting and documenting, 1021–1022
surveillance, 1019–1020
undercover investigations, 1020
Digital Millennium Copyright
Act (DMCA), 154
Digital Rights Management (DRM), 263–265
Digital Signature Algorithm (DSA), 357–358
Digital Signature Standard (DSS), 352, 357
digital signatures for message verification,
356–358
digital subscriber lines (DSLs), 648, 683–685

digital transmission, 644–645
digital video recording (DVR) systems, 913
digital zoom in CCTV systems, 915
dignitary wrongs category in civil law, 128
diode lasers in fiber-optic cable, 651
dips in electric power, 451
direct-attached storage for backups, 1038
direct sequence spread spectrum (DSSS),
562–563
directors of security operations in incident
response teams, 1001
directory permissions, testing, 821
directory roles in identity management,
748–750
directory services, 747–748
disassembly tools in forensics field kits, 1015
disaster recovery (DR)
availability issues, 1049–1053
description, 101, 1029–1030
incident response, 992
overview, 867–869
process overview, 1053–1055
disaster recovery plans (DRPs)
assessment, 1058
communications, 1056–1057
contents, 1055
description, 101
lessons learned, 1061
personnel, 1055–1056
responses, 1055
restoration, 1058–1060

disaster recovery plans (DRPs) (cont.)
storing, 1042
testing, 1061–1065
training and awareness, 1060–1061
disasters
business continuity, 1065–1071
business process recovery, 1033–1034
chapter questions, 1073–1076
chapter review, 1071–1073
data backups, 1034–1041
description, 1043
documentation, 1041–1042
human resources, 1042–1043
overview, 1029
reciprocal agreements, 1047–1048
recovery site strategies, 1043–1047
recovery strategies overview, 1029–1033
redundant sites, 1048–1049
disc tumbler locks, 919

discovery step in penetration testing, 824
discrepancies in identity, 798–799
discretionary access control (DAC)
challenges, 768
characteristics, 776
overview, 766–767
disposal of digital asset management, 262
disruption prevention in site planning, 424
distance-vector routing protocols, 535
distinguished names (DNs)
directory services, 747–748
LDAP, 749
distributed control systems (DCSs), 290, 293
distributed denial-of-service (DDoS) attacks
CDNs for, 674
DNS, 619–620
PaaS for, 303
Distributed Network Protocol 3 (DNP3),
626–627
distributed systems, 307–309
distribution facilities, 446–447
divestitures, 17–18
DKIM (DomainKeys Identified Mail), 625
DLP. See data loss prevention (DLP)
DMARC (Domain-based Message
Authentication, Reporting and
Conformance) system, 625
DMCA (Digital Millennium
Copyright Act), 154

DMZs (demilitarized zones) for firewalls
dual-homed, 959
functions, 945–946
screened subnet, 960
DNP3 (Distributed Network Protocol 3),
626–627
DNS. See Domain Name Service (DNS)
DNs (distinguished names)
directory services, 747–748
LDAP, 749
DNS over HTTPS (DoH), 621
DNSSEC (DNS security)
overview, 620–621
threats, 529–531
Do phase in Plan-Do-Check-Act loop, 875
DOCSIS (Data-Over-Cable Service Interface
Specifications), 687
documentation
audits, 839–840
backups, 863
change management, 262, 893
digital forensics, 1021–1022
disaster recovery, 1041–1042
forensics field kits, 1015

incident response, 992
software vulnerability scans, 901
DoDAF (Department of Defense Architecture
Framework), 173, 195
dogs, 929
DoH (DNS over HTTPS), 621
Domain-based Message Authentication,
Reporting and Conformance (DMARC)
system, 625
domain controllers (DCs) in directory
services, 747–748
domain generation algorithms (DGAs)
in DNS, 617–618
Domain Name Service (DNS)
attack prevention, 617–620
DNS over HTTPS, 621
DNSSEC, 620–621
domains, 526–527
filters, 621
MITRE ATT&CK framework, 389
overview, 524–526, 616
resolution components, 527–528
splitting, 530
threats, 529–531

⮝Index

DomainKeys Identified Mail (DKIM), 625
domains
collision and broadcast, 492–494
DNS, 526–527
doors
considerations, 437
data processing facilities, 443
lock delay feature, 920
types, 440–441
DoS (denial-of-service) attacks
STRIDE model, 388
wireless communications, 578
double-blind penetration tests, 826
double tagging attacks on VLANs, 632
downstream liability, 39, 161
downstream suppliers in risk management, 98
downtime in high availability, 1050
DPD (Data Protection Directive), 143
DPOs (Data Protection Officers)
in GDPR, 144
DR. See disaster recovery (DR)
draft IEEE 802.11i, 576
DRI International Institute, Professional
Practices for Business Continuity
Management, 106
drive-by downloads, 865

drives, self-encrypting, 407
DRM (Digital Rights Management), 263–265
dropped ceilings, 442
DRPs. See disaster recovery plans (DRPs)
dry pipe water sprinkler systems, 460
DSA (Digital Signature Algorithm), 357–358
DSD (dynamic separation of duty)
relations, 773
DSLAMs (DSL access multiplexers), 683
DSLs (digital subscriber lines), 648, 683–685
DSS (Deliver, Service and Support) domain in
COBIT 2019, 189
DSS (Digital Signature Standard), 352, 357
DSSS (direct sequence spread spectrum),
562–563
dual-attached concentrators (DACs)
in FDDI, 498
dual-attachment stations (DASs)
in FDDI, 498
dual control, 34
dual-homed firewalls, 959, 963
dual-use goods, 145

due care issues
disaster recovery plans, 1060
liability, 158–159
due diligence, 158–159
dumpster diving, 260–261
Dunn, Andy, 885
durability in ACID properties, 286
duress codes, 931–932
Dutch Data Protection Authority, 397
DVR (digital video recording)
systems, 913
Dyn attack, 307
dynamic analysis
antimalware software, 970
application security, 1139
dynamic application security
testing (DAST), 1139
Dynamic Frequency Selection (DFS), 574
Dynamic Host Configuration
Protocol (DHCP)
IP addresses, 501
overview, 517–519
dynamic mapping in NAT, 532
dynamic passwords, 729–732
dynamic ports, 507
dynamic routing protocols, 534–535
dynamic separation of duty (DSD)
relations, 773
Dyre Trojan, 604

E

E-carriers for WANs, 542
e-discovery, 236–237
e-mail
authorization, 624
DKIM, 625
DMARC, 625
gateways, 663
IMAP, 623–624
MIME, 625–626
overview, 621–622
phishing, 864
POP, 623
SPF, 624
threats, 623
E2EE (end-to-end encryption) vs. link
encryption, 600–602
EAC (electronic access control) tokens, 925

EAP (Extensible Authentication Protocol)
VPNs, 699
WPA Enterprise, 577
EAP and Transport Layer Security (EAPTLS), 580–581
EAP-TLS (Extensible Authentication
Protocol-Transport Layer Security)
authentication framework, 501
EAP-Tunneled Transport Layer Security
(EAP-TTLS), 580
ECC (elliptic curve cryptography),
328, 342–343
Economic Espionage Act, 141
economic wrongs category in civil law, 128
edge computing systems, 308–309
EDI (electronic data interchange), 538
EDLP (endpoint DLP), 273–274
EDM (Evaluate, Direct and Monitor) domain
in COBIT 2019, 189
EDNS(0) technique in DNS, 620
EDR. See endpoint detection
and response (EDR)
EDRM (Electronic Discovery
Reference Model), 237
EDU domain in DNS, 527
education. See training
EF (exposure factor), 74
effectiveness monitoring for risk, 91–92
egress
filtering, 948
monitoring, 981
80/20 Pareto principle, 179
802.1AE standard, 500–501
802.1AR standard, 501

802.1x standard, 579–581
802.11 standard, 565–566, 575–576
802.11a standard, 566–567
802.11ac standard, 567
802.11ax standard, 567–568
802.11b standard, 566
802.11e standard, 573
802.11f standard, 574
802.11g standard, 567
802.11h standard, 574
802.11i standard, 576–578
802.11j standard, 574
802.11n standard, 567
802.11w standard, 578

802.15.4 standard, 570–571
802.16 standard, 569
EIGRP (Enhanced Interior Gateway
Routing Protocol), 536
EKs (endorsement keys) in Trusted
Platform Modules, 405
Elastic Stack product, 979
electric power
backup, 448–450
considerations, 438
fallback plans, 448
issues, 450–452
overview, 670–672
protecting, 452–453
electrical wires in transmission media, 643
electromagnetic analysis for smart cards, 735
electromagnetic interference (EMI)
coaxial cable, 649
electric power, 450
electromechanical IDSs, 926
electronic access control (EAC) tokens, 925
electronic data interchange (EDI), 538
Electronic Discovery Reference Model
(EDRM), 237
electronic monitoring of passwords, 721
electronic vaulting for backups, 1038–1039
electronically stored information (ESI),
236–237
elevation of privilege category in STRIDE
model, 388
elliptic curve cryptography (ECC), 328,
342–343
embedded systems, 306
Embedding Business Continuity practice in
Good Practice Guidelines, 105
emergency category in PACE plans, 1057
emergency changes, 892
emergency management, 931
emergency response groups, 1057

emergency response procedures, 868–869
EMI (electromagnetic interference)
coaxial cable, 649
electric power, 450
Emotet Trojan, 604
employees. See personnel safety and security
emtocells in Li-Fi standard, 568
emulating services in honeypots, 974
emulation buffers in antimalware, 970

🡑Index

Encapsulating Security Payload (ESP), 608
encapsulation
multilayer protocols, 628
object-oriented programming, 1127–1128, 1130
OSI, 472–473
TCP, 509
encryption. See also cryptology
bus, 407–408
code repositories, 1144
data at rest, 255
data in motion, 255–256
homomorphic, 258
hybrid methods, 346–350
Internet of Things, 307
Kerberos, 785–789
link vs. end-to-end encryption, 600–602
meeting applications, 694
mobile devices, 243
network sockets, 703
overview, 256–258
passwords, 722
end-of-life (EOL) of assets, 229
end-of-support (EOS) of assets, 229
end-to-end encryption (E2EE) vs. link encryption, 600–602
end-user environment in business continuity planning, 1071
End User License Agreement (EULA), 153
endorsement keys (EKs) in Trusted Platform Modules, 405
endpoint detection and response (EDR)
breach attack simulations, 828
defense in depth, 391
effectiveness monitoring, 91–92
HIDSs, 968
security operations centers, 940
endpoint DLP (EDLP), 273–274
endpoint security, 673–674