Microsoft®

CISSP Rapid Review

Darril Gibson

Rapid Review

CISSP Exam

Assess your readiness for the Certified Information Systems Security Professional (CISSP) exam—and quickly identify where you need to focus and practice. This practical, streamlined guide walks you through each exam objective, providing “need to know” checklists, review questions, tips, and links to further study—all designed to help bolster your preparation.

Reinforce your exam prep with a *Rapid Review* of these objectives:

- Access Control
- Telecommunications and Network Security
- Information Security Governance & Risk Management
- Software Development Security
- Cryptography
- Security Architecture & Design
- Operations Security
- Business Continuity & Disaster Recovery Planning
- Legal, Regulations, Investigations, and Compliance
- Physical (Environmental) Security

This book is an ideal complement to the in-depth training of the Microsoft Press® *Training Kit* for the CISSP Exam and other exam-prep resources.

ABOUT THE AUTHOR

Darril Gibson regularly teaches, writes, and consults on a wide range of security and technical topics. He holds several certifications including MCT, MCSA, MCSE, A+, Network+, Security+, and CISSP. Darril has written more than 20 books, including several popular certification titles.

SERIES EDITOR

Orin Thomas, MCITP, MCTS, MCSE, Microsoft MVP

microsoft.com/mspress

ISBN: 978-0-7356-6678-8

9 780735 666788 90000

U.S.A. $29.99
Canada $31.99
[*Recommended*]

Certification/CISSP

Microsoft®

Microsoft®

CISSP Rapid Review

Darril Gibson

ISBN: 978-0-7356-6678-8

1 2 3 4 5 6 7 8 9 LSI 7 6 5 4 3 2

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Microsoft and the trademarks listed at *http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx* are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions and Development Editor: Kenyon Brown
Production Editor: Rachel Steely
Editorial Production: nSight, Inc.
Technical Reviewer: Andrew Brice
Copyeditor: Richard Carey
Indexer: Nancy Guenther
Cover Design: Best & Company Design
Cover Composition: Zyg Group, LLC
Illustrator: Rebecca Demarest

Contents at a Glance

Contents

Introduction

This Rapid Review is designed to assist you with studying for the (ISC)^2 CISSP exam. The Rapid Review series is designed for exam candidates who already have a good grasp of the exam objectives through a combination of experience, skills, and study and could use a concise review guide to help them assess their readiness for the exam.

The CISSP exam is aimed at an IT security professional who has a minimum of five years of direct full-time security work experience in two or more of the 10 domains of the (ISC)^2 CISSP Common Body of Knowledge (CBK). One year can be waived for certain college degrees and technical certifications.

Candidates who take this exam should have the knowledge and skills required to do the following:

- Identify risk and participate in risk mitigation activities
- Provide infrastructure, application, operational, and information security
- Apply security controls to maintain confidentiality, integrity, and availability
- Identify appropriate technologies and products
- Operate with an awareness of applicable policies, laws, and regulations

It is important to note that real-world experience with security is required prior to earning the CISSP certification and that having practical knowledge is a key component to achieving a passing score.

This book reviews every concept described in the following exam objective domains:

- 1.0 Access Control
- 2.0 Telecommunications and Network Security
- 3.0 Information Security Governance & Risk Management
- 4.0 Software Development Security
- 5.0 Cryptography
- 6.0 Security Architecture & Design
- 7.0 Operations Security
- 8.0 Business Continuity & Disaster Recovery Planning
- 9.0 Legal, Regulations, Investigations and Compliance
- 10.0 Physical (Environmental) Security

This is a Rapid Review and not a comprehensive guide such as the forthcoming *CISSP Training Kit* (Microsoft Press, 2013). The book covers every exam objective on the CISSP exam but will not necessarily cover every exam question. (ISC)^2 regularly adds new questions to the exam, making it impossible for this (or any) book to provide every answer. Instead, this book is designed to supplement your existing independent study and real-world experience.

If you encounter a topic in this book with which you do not feel completely comfortable, you can visit the links described in the text in addition to researching the topic further by using other websites, as well as consulting support forums.

NOTE **The Rapid Review is designed to assess your readiness for the CISSP exam. It is not designed as a comprehensive exam preparation guide. If you need that level of training for any or all of the exam objectives covered in this book, we suggest the forthcoming *CISSP Training Kit* (ISBN: 9780735657823). The Training Kit will provide comprehensive coverage of each CISSP exam objective, along with exercises, review questions, and practice tests. The Training Kit will also include a discount voucher for the exam.**

(ISC)^2 professional certification program

(ISC)^2 professional certifications cover the technical skills and knowledge needed to succeed in different IT careers. The CISSP certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge and is used by organizations and professionals around the globe. (ISC)^2 CISSP certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. (ISC)^2 exam objectives reflect the subject areas in an edition of an exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional with a number of years of experience.

MORE INFO **For a full list of (ISC)^2 certifications, go to** *https://www.isc2.org/credentials/.*

Acknowledgments

Books like this are never by just one or two people but instead are created with the combined efforts of a large group of people. I'm grateful for the help and support I received from multiple individuals at O'Reilly and Microsoft Press. I'm especially grateful for the outstanding technical input provided by Andrew Brice, the technical editor.

Support & feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site: http://www.microsoftpressstore.com/*title/9780735666788*

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority and your feedback our most valuable asset. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the Exam

Certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Rapid Review and another training kit for your "at home" preparation and take an (ISC)^2 CISSP professional certification course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 1

Access control

The Access Control domain covers a variety of different controls used to identify subjects, authenticate them, and control the access they are granted to different objects by controlling rights and permissions. Audit trails are an important element of accounting and logging and, combined with effective authentication, provide individual accountability. Access control attacks are common, and it's important for security professionals to have a basic understanding of evaluating threats and analyzing vulnerabilities to determine overall risk. Ideally, access controls are implemented to fully support an organization's security policy, and a way to verify this is through access reviews and audits. These reviews and audits can also detect problems in the identity and access provisioning life cycle, such as inactive accounts that have not been disabled.

This chapter covers the following objectives:

- Objective 1.1: Control access by applying the following concepts/methodologies/techniques
- Objective 1.2: Understand access control attacks
- Objective 1.3: Assess effectiveness of access controls
- Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

Objective 1.1: Control access by applying the following concepts/methodologies/techniques

For this exam objective, you must understand many of the basics related to IT risk management. Security policies provide overall direction for an organization. Personnel within the organization then implement different types of controls to support the policy. At the core of access control is effective authentication, and it's important to understand the authentication factors. Without effective authentication, it isn't possible to enforce authorization and data within audit trails is not useful. Single sign-on (SSO) authentication methods have been widely available within a single organization's environment, but newer methods support SSO in federations. You should have an understanding of federated identity management systems and some of the XML-based protocols that they use to share authentication information.

Exam need to know...

- Policies
  For example: Do you know and understand the common elements of a security policy, such as the principle of least privilege and separation of duties? What is an acceptable use policy?
- Types of controls (preventive, detective, corrective, and so on)
  For example: What type of control is an audit trail? What type of control is a security guard?
- Techniques (for example, non-discretionary, discretionary, and mandatory)
  For example: What is a commonly used non-discretionary model that organizes users into groups?
- Identification and authentication
  For example: One authentication method requires users to enter a password and a PIN. Another model requires users to use a smart card and a PIN. Which is stronger?
- Decentralized/distributed access control techniques
  For example: What XML-based standards are used to provide SSO capabilities in a federated identity management system?
- Authorization mechanisms
  For example: How does a constrained user interface control access? What are the differences among an access control list, a capability table, and an access control matrix?
- Logging and monitoring
  For example: What is provided by an audit trail? What is included in log management?

Policies

At the heart of any access control strategy is one or more security policies that identify the overall security goals of an organization. The security policy provides a high-level overview of generalized goals, and it is used to create more specific guidelines, standards, and procedures. Security policies commonly include one or more of the following elements:

- An acceptable use policy (AUP) informs users of their responsibilities when using IT systems and identifies unacceptable behaviors. Users should reread and acknowledge the AUP periodically, such as once a year.
- Least privilege refers to the practice of granting subjects access only to what they need to perform their jobs and no more.
- A separation of duties policy ensures that no single entity can control an entire process. It helps prevent fraud by requiring two or more people to conspire together.
- Job rotation policies help prevent fraud by ensuring that a person does not remain in the same position for an extended period and gain excessive control over any area of the business.

Access Control policies commonly refer to subjects and objects. A subject (such as a user) can access an object (such as a file or other resource). Subjects are often grouped together by using roles or groups to simplify administration. Similarly, objects are also grouped together, such as grouping files within folders or shares to simplify administration. As a best practice, permissions for an object are rarely granted to a single subject.

True or false? The primary goal of security policies is to protect confidentiality, integrity, and availability of an organization's assets.

Answer: *True*. Security policies and procedures are in place to support the core security goals of preventing the loss of confidentiality, integrity, or availability of assets.

> ***EXAM TIP*** **Often a question can sound overly complex when it is referring to *subjects* and *objects,* but you can usually simplify it by substituting the word *users* for *subjects* and the word *files* for *objects*. For example, instead of "Access Control administration is simplified by grouping subjects and objects," you can think of this as "Access Control administration is simplified by grouping users and files." Subjects can be more than just users, and objects can be more than just files, but substituting subjects with users and objects with files works in many instances without changing the meaning.**

> ***MORE INFO*** **The Operations Security domain (covered in Chapter 7, "Operations security") specifically mentions some security operations concepts, such as need-to-know, least privilege, separation of duties, and job rotation. Overall, you'll find that many of the Access Control topics have some similarities to the Operations Security topics.**

Types of controls (preventive, detective, corrective, and so on)

Security controls are safeguards or countermeasures put into place to reduce overall risk. One way they are classified is based on how they are implemented:

- **Technical or logical** controls are implemented with technology such as protecting objects with permissions or requiring users to change their passwords with a technical password policy.
- **Physical** controls include elements that you can physically touch, such as a door lock or a closed circuit television (CCTV).
- **Administrative or management** controls are written security policies or methods used to check the effectiveness of security, such as assessment or audit.

True or false? Pre-employment background investigations are a type of administrative control.

Answer: *True*. This is a procedure and would be done based on a policy.

Another way controls are classified is based on what they do, and they are often grouped together with the implementation method. Control classifications include the following:

- **Preventive** controls attempt to prevent incidents before they occur. A firewall is a technical preventive control because it can prevent malicious traffic from entering a network. A guard is a physical preventive control. Administrative preventive controls include access reviews and audits.
- **Detective** controls identify security violations after they have occurred, or they provide information about the violation as part of an investigation. An intrusion detection system is a technical detective control, and a motion detector is a physical detective control. Note that both an intrusion detection system and a motion detector include the word "detect," which is a good clue. Reviewing logs or an audit trail after an incident is an administrative detective control.
- **Corrective** controls attempt to modify the environment after an incident to return it to normal. Antivirus software that quarantines a virus is an example of a technical corrective control. A fire extinguisher is an example of a physical corrective control.
- **Deterrent** controls attempt to discourage someone from taking a specific action. A high fence with lights at night is a physical deterrent control. A strict security policy stating severe consequences for employees if it is violated is an example of an administrative deterrent control. A proxy server that redirects a user to a warning page when a user attempts to access a restricted site is an example of a technical deterrent control.
- **Directive** controls are administrative controls that provide direction or guidance.
- **Compensating** controls are controls used as alternatives to the recommended controls. NIST SP800-53 mentions a compensating control used for an industrial control system (ICS). A change management policy might dictate the testing of all updates on live systems prior to deployment, but this might not be feasible for an ICS. A compensating control is an offline replicated system used for testing.
- **Recovery** controls provide methods to recover from an incident.

True or false? A user entitlement access review and audit is a detective control.

Answer: *False*. It is a preventive control. It is designed to identify whether users have more privileges than necessary prior to an incident. Discrepancies in assigned privileges can be corrected to prevent an incident. If an incident had already occurred, reviewing an audit trail would be a detective control.

EXAM TIP **Given a security control, you should be able to identify it as preventive, detective, corrective, deterrent, recovery, or directive in nature. For example, visible security controls are deterrent in nature because they deter attackers. You should also be able to identify it as technical, physical, or administrative. For example, motion-activated lights are a physical preventive control.**

MORE INFO **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Information Security," provides in-depth coverage of security controls. You can download it from this page: *http://csrc.nist.gov/publications/PubsSPs.html*. NIST SP 800-53 organizes the controls in families and classes that don't directly relate to the CISSP types of preventive, detective, and corrective, but the document does provide excellent descriptions and information about usage of IT security controls.**

Techniques (non-discretionary, discretionary, and mandatory)

Non-discretionary access controls are centrally managed, and discretionary access controls (DAC) are managed by data owners. Mandatory access controls (MACs) are predefined by a higher authority, such as a policy that defines access labels.

In a DAC model, every object is owned by a subject and the owner has full control over the object. For example, when a user creates a file, the user owns the file and can modify the permissions. Common operating systems such as Windows and Linux use the DAC model.

In non-DAC models, subject and object access is controlled centrally, such as by an administrator. Role-Based Access Control (RBAC) is a common example in which subjects are placed into roles or groups by administrators. Access to objects is granted to the roles rather than to individuals.

True or false? Access control administration is simplified by grouping subjects and grouping objects.

Answer: *True*. Users and other subjects are often grouped together by using an RBAC model. Similarly, objects such as files are often grouped together in folders and shares.

EXAM TIP **Know the primary differences between the models. DAC grants full control to end users. MAC uses predefined rules and labels to grant access. RBAC is a non-discretionary model that is controlled by administrators.**

MAC uses labels assigned to subjects and objects, and when the labels match, subjects are granted access. Labels can be assigned in a hierarchical environment such as Unclassified, Secret, and Top Secret, with higher-level authorization also providing access to lower-level classifications. For example, someone granted Top Secret access also has Secret access. Labels can be assigned in a compartmentalized environment where access to one compartment does not provide access to any other data. A hybrid model uses compartments within classification levels and is easier to manage.

True or false? The Bell-LaPadula model is an example of a MAC model.

Answer: *True*. It uses a basic rule of no read up, no write down. The Simple Security Rule states that a subject cannot read up, and the *-property (star property) rule states that a subject cannot write down. In contrast, the Biba model (which is also a MAC model) uses a Simple Integrity Axiom of no read down and a * (star) Integrity Axiom of no write up.

EXAM TIP **Different access control models have different primary goals. For example, the Bell-LaPadula model has a primary focus of ensuring confidentiality (ensuring that unauthorized users cannot access data). The Biba model has a primary focus on integrity (ensuring that unauthorized modification of data does not occur). The Clark-Wilson model and the Chinese Wall (also called Brewer-Nash) model use strict separation of duties rules to enforce integrity.**

Identification and authentication

Identification occurs when a user claims an identity, such as with a user name. Authentication occurs when the user proves the claimed identity by using one or more factors of authentication. The three primary factors of authentication are as follows:

- Something you know (such as a password or PIN)
- Something you have (such as a smart card or RSA token)
- Something you are (proven with biometrics)

You can combine two or more factors to provide stronger authentication. Two-factor authentication uses a method in two of the categories and is stronger than using a single factor. Multifactor authentication uses methods in two or more categories.

Even though passwords are usually stored as a hash, they can be cracked by using common comparative analysis tools. If attackers can access a password database, they can perform an offline analysis and quickly crack the passwords. Rainbow tables are commonly used in these attacks. Salting the hash with random bits protects against many offline password attacks, including the use of rainbow tables.

MORE INFO **A hashing algorithm provides one-way encryption of data, creating a unique fixed-size string. Strong hashing algorithms such as SHA-256 are resistant to collisions, meaning that it is not feasible to identify another input to create the same hash. In this case, it would be difficult to identify another password that creates the same hash so that a successful comparative analysis discovers the original password. Salts thwart rainbow table attacks, but other attacks, such as dictionary attacks or brute-force attacks, can still be successful against an offline database of passwords.**

True or false? Using a PIN and a password is an example of multifactor authentication.

Answer: *False*. A personal identification number (PIN) and a password are both in the same authentication factor (something you know). This is one-factor authentication, not multifactor authentication.

EXAM TIP **Know the differences between the authentication factors. Passwords are the weakest form of authentication, but combining passwords with a method in a different factor, such as a smart card or using biometrics, provides multifactor authentication and increases the strength. Some specific access methods require stronger authentication. For example, remote access connections are vulnerable to attack, and multifactor authentication makes it more difficult for an attacker to impersonate a user.**

Biometrics provide strong authentication, but they are susceptible to both false positives and false negatives. A false positive presents the highest risk. This occurs when an unauthorized individual is incorrectly identified as being authorized. The accuracy of a biometric system is identified by the crossover error rate (CER), which is calculated from Type 1 errors (false rejections) and Type 2 errors (false positives). A lower CER indicates a more accurate biometric system.

A simple way to reduce the risk of Type 1 and Type 2 errors is to use two-factor authentication. For example, in addition to the biometric method, the user can also be required to use a password.

A similar concept is used with credit cards and online purchases. Instead of just requiring the user to provide the credit card number and expiration date, users are often required to provide the credit card verification code. This is a 3-digit or 4-digit number on the front or back of the card.

True or false? Between iris scanners and retinal scanners, iris scanners are the most accurate form of biometric authentication.

Answer: *False*. Retinal scans are the most accurate form of biometric authentication. Even identical twins will have identifiable differences.

> ***EXAM TIP*** **Biometric authentication is the strongest form of authentication. Retinal scans measure the blood vessels in the back of the eye and are the most accurate method. Fingerprints are the most common method of biometrics in use.**

Single sign-on (SSO) techniques are used in several different access control and identity management systems. These allow a user to log on once and access multiple resources without logging on again.

Internal networks can use a database such as Microsoft's Active Directory to manage user identities and provide SSO. Regular users have a single account and can access any resources in the network as long as they have permissions.

Kerberos is commonly used as an authentication protocol in a centralized model. It requires a central database of accounts and synchronized time (ideally synchronized with an external time source). Kerberos uses time-stamped tickets to authenticate accounts when they try to access a resource. These tickets are encrypted with symmetric encryption. Early versions of Kerberos used Data Encryption Standard (DES), which is now considered cracked, and current versions use Advanced Encryption Standard (AES).

> ***EXAM TIP*** **Know that SSO is part of an identity management system and can be used in a centralized environment such as a Microsoft domain using Kerberos. SSO methods are also implemented in federated identity management systems that include different operating systems.**

Remote access protocols provide authentication, authorization, and accounting (AAA) services. Some common AAA protocols include the following:

- **Terminal Access Controller Access-Control System (TACACS)** One of the first AAA protocols used with remote access systems, TACACS has been replaced by RADIUS, TACACS+, or Diameter in most situations. TACACS uses UDP port 49 by default.
- **Remote Authentication Dial-in User Service (RADIUS)** This is a widely used AAA protocol in remote access systems and by Internet service providers (ISPs). It is used with both dial-in and virtual private network (VPN) access. It uses UDP and encrypts the password but not the entire authentication session.
- **TACACS Plus (TACACS+)** Cisco created this as a proprietary upgrade to TACACS. It separates each element of AAA in three processes. In comparison, RADIUS combines authentication and authorization. TACACS+ uses TCP port 49 instead of UDP, and it encrypts the entire authentication session instead of just the password.
- **Diameter** This is an alternative or upgrade to RADIUS, and it has much more flexibility. It can be used with wireless devices, Voice over IP (VoIP), Mobile IP, and smartphones, but it is not backward-compatible with RADIUS. The name implies it is twice as good as RADIUS because the diameter of a circle is twice the length of the radius.

EXAM TIP **Common remote access protocols are RADIUS, TACACS+, and Diameter. TACACS+ is proprietary to Cisco and includes several benefits over RADIUS. Diameter has the most flexibility.**

MORE INFO **RADIUS is defined in RFC 2865 and has been updated by 2868, 3575, and 5080. Diameter is defined in RFC 3588. By replacing *xxxx* with the RFC number, you can view any RFC with the following URL: *http://tools.ietf.org/html/rfcxxxx*. TACACS+ is not defined in a formal RFC, but it is documented in a draft document available here: *http://tools.ietf.org/html/draft-grant-tacacs-02*.**

Decentralized/distributed access control techniques

Distributed computing environments (DCEs) use distributed SSO mechanisms to control access. Federated identity management systems are used to provide SSO to Internet users from different entities. In this context, a federation is a group of companies that decide they want to collaborate to share resources.

For example, imagine that employees in Company A are granted access to resources in Company B and Company C. Instead of requiring these users to have three separate passwords, they can log on once within Company A and then access resources in Company B and Company C without logging on again.

MORE INFO **The MSDN article "Federated Identity: Scenarios, Architecture, and Implementation" includes excellent examples of when a federated identity management system is needed and of some of the challenges. You can access it here: *http://msdn.microsoft.com/library/aa479079.aspx*.**

A significant challenge is sharing the authentication and authorization information between the companies. If everyone used the same technologies, it would be easier to share the data, but more often, the federation has a heterogeneous identity environment. Different companies use different identity management methods.

Standards based on Extensible Markup Language (XML) are often used to share federated identity information over the Internet. Some of the commonly used standards include the following:

- Security Assertion Markup Language (SAML), which includes both authentication and authorization information
- Service Provisioning Markup Language (SPML), which is used to share provisioning information between organizations in the federation
- Extensible Access Control Markup Language (XACML), which provides a standard for evaluating authorization requests

True or false? SAML is used to provide SSO access when users are accessing sites with web browsers.

Answer: *True*. SAML is one of the schemas used with federated access, and it is often used to provide access via web browsers.

EXAM TIP **A federated identity is an SSO-based identity that is portable between different organizations within a federation. Federated identity management systems use HTML-based and XML-based languages to share authentication and authorization information with each other. Many e-commerce solutions have implemented federated identity management systems to streamline the customer experience when making purchases from partner companies in a federation.**

MORE INFO **There are several resources on SAML, SPML, and XACML that you might find valuable. "Demystifying SAML" is available here: *http://www.oracle.com/technetwork/articles/entarch/saml-084342.html*. "XACML Overview" is available here: *http://xml.coverpages.org/xacml.html*. The full SPML v2.0 specification can be downloaded here: *http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip*.**

Authorization mechanisms

After subjects prove their identity, or authenticate, they are granted access to objects based on their proven identity. Most authorization systems start with an implicit deny philosophy. For example, a user is denied access to files and folders unless the user is specifically given permissions to access them.

A common type of access model is RBAC, in which users are placed into roles or groups and privileges are granted to the group. However, there are other authorization mechanisms that can be used either separately or in combination with an RBAC model.

A constrained user interface limits what the user can see or do based on the user's privileges. For example, imagine an application that can be used by both administrators and regular users. When administrators use it, all the menu items are visible and the application has full functionality. When a regular user starts the application, the menu items are either hidden or dimmed so that they can't be selected. When menu items are hidden, the users are unaware of the advanced capabilities.

Databases commonly use views as a constrained user interface to limit the available data. For example, an employee table might include names, addresses, phone numbers, and salary data. One view might include only names and phone numbers, and another view might include names and salary data. Users are granted access to the view that shows data that they're authorized to view, but they are not granted access to the other view or the underlying table.

Temporal-based authorization controls limit access based on time. For example, a virtual private network (VPN) user might be authorized to connect any weekday between 7:00 A.M. and 7:00 P.M. If the user attempts to connect on a weekend, the connection is blocked.

Location-based authorization controls limit access to specific locations. For example, an employee might be authorized to work from home by using a dial-in connection. Caller ID or callback technologies can be used to ensure that the user is calling from home and that another user is not impersonating the user from another location.

An extension of this is location-based authorization controls using domains. For example, the United States government purchased antivirus (AV) software for all government employees that they can download for free. The AV vendors restrict access to the download websites to allow only traffic coming from .mil domain locations.

Access control lists (ACLs), capability tables, and access control matrices (ACM) are related. An ACL is directly associated with an object, a capability table is directly associated with a subject, and an ACM combines them both. For example, a folder named data (an object) includes an ACL that lists all users granted access to the folder and their specific levels of access, such as read or write. A capability table might be created for a user named Darril (the subject) and include a list of all folders that he can access. The ACM includes all objects and all subjects and can be quite large.

NOTE **ACLs are commonly associated with routers as a list of IP addresses, ports, and protocol IDs that are allowed in or out of a network. In this context, the router is the object and the IP address, port, or protocol ID is the subject. An ACL is created for each router, defining the access for different subjects (IP addresses, ports, or protocol IDs). A capability model might be created for different protocols, such as File Transfer Protocol (FTP), and list all routers that allow FTP traffic. An ACM would include all routers and all protocols.**

True or false? The security kernel of an operating system controls access between subjects and objects.

Answer: *True*. A security kernel controls access. For example, the Windows kernel-mode security reference monitor in current Windows–based systems uses discretionary ACLs (DACLs) to determine access with the DAC model.

> ***EXAM TIP*** **Know the differences among an ACL, a capability table, and an ACM. The ACL is focused on an object and lists subjects that can access it. The capability table is focused on a subject and lists objects the subject can access. The ACM combines them both.**

Logging and monitoring

Logs record activity as it occurs and record details such as who did it (which account), what happened, when it happened, and where it happened. You can use one or more audit logs to create an audit trail. An audit trail is a detective control and provides enough information so that you can identify the relevant events leading up to and during an incident.

Audit trails are required to ensure accountability and depend on effective identification and authorization techniques. If users can easily use another account, the audit trail cannot effectively identify who took an action.

Log management methods ensure that logs are maintained to provide a full audit trail, that the logs are protected from modification, and that they are regularly reviewed. Protecting logs from modification is especially important if they will be used as evidence in court. Access to the logs should be restricted to administrators and security personnel only.

Administrators also use logs to manage and maintain systems. They provide key information used during troubleshooting and recovery of systems after a failure. These logs are used to help prevent or minimize loss of availability.

True or false? Audit trails are a type of preventive control that record who took an action, what action the user took, and when the user took it.

Answer: *False*. Audit trails are a type of detective control. An audit trail logs events as they occur, including details on who, what, when, and where. After an incident has occurred, these logs can be examined to re-create the events.

> ***EXAM TIP*** **Log management includes the practice of reviewing the logs (either manually or with an automated system) and protecting the logs from modification after they've been created. Logs should be synchronized with an external time source so that all logs record the same time. They should be stored in a central location that has restricted access. Attackers will often try to erase their recorded activity, but this is more difficult if the log is stored in another location.**

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are also used for logging and monitoring. An IDS is a detective control that can detect attacks, and an IPS is a preventive control that can prevent attacks by detecting and blocking them before they reach an internal network. Both controls send alerts or some type of notification when they detect a potential attack.

However, each alert isn't necessarily an attack. IDSs have adjustable thresholds, and an alert is created only when activity exceeds the threshold. If the threshold is too high, actual attacks can get through undetected. If the threshold is too low, the system generates too many false positives.

True or false? An IPS is placed in line with traffic.

Answer: *True*. All traffic goes through an IPS. The IPS detects and blocks malicious traffic but allows safe traffic through to the network.

> ***MORE INFO*** **IDSs and IPSs are mentioned in the Operations Security domain in Chapter 7, including methods of detection and response.**

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. An organization has created a high-level document designed to provide direction to employees about security within the organization. What is this?
2. An audit trail is being used to identify events leading up to a security incident. What type of control is an audit trail in this situation?
3. What is the difference between an ACL and an ACM?
4. What is a measure of a secure biometric authentication system?
5. What is the purpose of SAML?
6. What type of authorization mechanism is a database view?
7. An audit trail is used after an incident. What is required for this audit trail to support individual accountability?

Objective 1.2: Understand access control attacks

Risk is identified by calculating the probability that a threat will exploit a vulnerability. Often, the threats come in the form of attackers attempting to exploit vulnerabilities in an organization's people, processes, or technology. Risk management includes identifying threats by using threat modeling, identifying valuable assets to protect, and analyzing vulnerabilities. Risks can then be mitigated with controls that reduce the impact of threats or reduce vulnerabilities.

Exam need to know...

- Threat modeling
  For example: What are some methods of social engineering? What's the difference between a denial of service (DoS) and a distributed denial of service (DDoS) attack?

- Asset valuation
  For example: When should the value of assets be identified? What assets should be evaluated within an organization as part of a risk management process?
- Vulnerability analysis
  For example: How often should vulnerability assessments be done? What can a vulnerability scan detect?
- Access aggregation
  For example: What types of attacks are launched by Advanced Persistent Threats (APTs)? Who can be a target of an APT?

Threat modeling

Threat modeling is the process of identifying potential and realistic threats to an organization's assets. You should be aware of common methods of access control attacks, including the following:

- **Social engineering** Attackers can often gain access simply by asking. This includes in-person, over the phone, and via email such as with phishing, spear-phishing, and whaling. It can also include tailgating and shoulder surfing.
- **Dumpster diving** If papers are thrown in the trash, they can easily be retrieved to gain information.
- **Malware** Viruses, worms, Trojan horses, and logic bombs are common methods that attackers use to gain control of a system or launch access control attacks.
- **Mobile code** Attackers have hijacked legitimate websites and installed malicious ActiveX and Java scripts. This represents a threat to the organization hosting the website. Additionally, visitors can be attacked by a drive-by download.
- **Denial of Service (DoS)** These come from a single attacker and attempt to disrupt normal operation or service of a system. A classic DoS attack is the SYN flood attack. DoS attacks are commonly launched against Internet-facing servers (any server that can be reached by another public IP address).
- **Distributed DoS (DDoS)** These come from multiple attackers, such as zombies in a botnet.
- **Buffer overflow** When input validation isn't used, unexpected code can cause an unhandled error and allow an attacker to install malicious code on a system.
- **Password crackers** Applications are widely available that can crack a password through comparative analysis. If the attacker can gain access to a database with passwords, the attacker can crack the passwords offline.
- **Spoofing** Attackers attempt to impersonate others in many different ways. They can spoof IP addresses, MAC addresses, and email addresses. Similarly, masquerading is when a social engineer impersonates someone such as a repairman.

- **Sniffers** Protocol analyzers placed on a network can capture traffic for later analysis. If passwords or valuable data are sent unencrypted, they can easily be read. Sniffers are often used in man-in-the-middle and replay attacks.
- **DNS-related attacks** Users can be tricked into providing their credentials on a bogus website after a DNS poisoning attack redirects traffic. DNS poisoning is used in pharming attacks.

True or false? Executives can be targeted through a whaling attack.

Answer: *True*. Whaling is a form of phishing that targets executives such as CEOs, presidents, and vice presidents.

True or false? A SYN flood attack uses spoofed IP addresses and causes a buffer overflow.

Answer: *False*. A SYN flood attack commonly uses spoofed IP addresses, but it doesn't cause a buffer overflow. Instead, it disrupts the three-way TCP handshake process by holding back the third packet.

> ***EXAM TIP*** **Know the common methods of attacks and the methods used to mitigate them. For example, the best prevention against social engineering is education, malware is detected and isolated with up to date antivirus software, and many DoS and DDoS attacks can be detected or prevented with IDSs or IPSs.**

> ***MORE INFO*** **Attacks come from multiple sources. In "Rethinking the Cyber Threat - A Framework and Path Forward," Scott Charney of the Microsoft Trustworthy Computing Group outlines four categories: conventional cybercrimes, in which attackers target systems for criminal purposes; military espionage, in which nation states sponsor attacks against military targets to obtain military secrets; economic espionage, in which intellectual property is stolen for economic gain; and cyber warfare, in which attackers attempt to disrupt or disable the IT services of an enemy. You can download the white paper here: *http://www.microsoft.com/download/details.aspx?id=747*.**

Asset valuation

One of the first steps in risk management is identifying the value of assets within the organization. This includes hardware assets, software assets, data and information assets, system assets, and personnel assets.

Key steps within the risk management process depend on knowing the value of the assets. For example, a cost-benefit analysis helps determine the return on investment (ROI) of a control. The ROI is high if you purchase an effective control for US$1,000 to protect a web farm generating 1 million dollars a day. It is ridiculously low if you pay US$1,000 to protect a US$15 keyboard. These examples represent two extremes where the answer is obvious, but the answers aren't always so clear, especially if the value of assets is not known.

True or false? Asset valuation is done only on hardware assets.

Answer: *False*. Asset valuation should be done on all assets, including hardware, software, data or information, and personnel. Many systems, such as a web farm, include hardware, software, and data and represent a combined value much greater than that of their individual components.

> ***EXAM TIP*** **Identifying the value of assets is an important first step in risk management and requires input from management. Technicians managing systems don't necessarily realize how much money a system generates, and without guidance, they might give the same amount of attention to a simple file server as they do to a server generating millions in revenue.**

Vulnerability analysis

A vulnerability analysis helps determine how vulnerable a system is to one or more threats. This is often referred to as two separate processes: vulnerability scans and vulnerability assessments.

Vulnerability scans are performed with automated tools such as Nmap to determine what vulnerabilities exist at any given time. Vulnerability scanners can detect a wide assortment of vulnerabilities, including open ports, unpatched or misconfigured systems, and weak passwords.

A vulnerability assessment is an overall examination of the organization beyond just a technical scan. It will often attempt to match threats with vulnerabilities and use available data to determine the likelihood or probability that a threat will attempt to exploit a vulnerability. Data reviewed in an assessment includes security policies, historical data on past incidents, audit trails, and the results of various tests, including vulnerability scans.

Threats and the environment regularly change, so these reviews and scans must be repeated. Based on their security policies and available resources, organizations must decide how often to repeat the vulnerability scans and assessments. For example, a large organization might perform vulnerability scans weekly and vulnerability assessments annually, but a smaller organization might do scans only monthly.

True or false? Risk management is an ongoing process, and a vulnerability analysis is a point-in-time assessment.

Answer: *True*. Risk management is a continuous process that needs regular attention. A vulnerability analysis identifies vulnerabilities at a given time, but changes in threats or the environment negate the findings.

> ***EXAM TIP*** **Controls are put into place to support an organization's security policies. Vulnerability assessments and scans evaluate the effectiveness of these controls.**

Access aggregation

Access aggregation refers to the combination of methods used to gain progressively more and more access. As a basic example, malware often attempts to progressively increase its privileges until it has full administrative access. On a larger scale, attackers often use a combination of methods to gain more and more access to an organization.

For example, an attacker might decide to target an organization and start with a dozen or so social engineering phone calls. Each call gets one more piece of information, and eventually the attacker has the names and email addresses of several executives. He might then use whaling to send one or more malware-infected phishing emails to these executives. If one of the executives takes the bait, the malware begins collecting information and sending it to the attacker.

This is challenging enough if you are considering only one attacker. Advanced Persistent Threats (APTs) are composed of full teams of attackers. They often have unlimited funding from a nation-state sponsor, but they could just as easily be funded by any group that has the money and a target.

True or false? An APT is a group of attackers, often sponsored by a government, that attacks only military or government targets.

Answer: *False*. An APT is often sponsored by a government, but it can target any organization. Attacks against organizations such as Google and Lockheed Martin are believed to have come from APTs.

> ***EXAM TIP*** **Attacks previously were primarily opportunistic, where the attackers looked for easy targets. When they failed to breach a target, they moved on to an easier one. In contrast, APTs launch targeted attacks against specific organizations and are not deterred by initial failures. They are often composed of state-sponsored personnel and use a wide variety of attack methods to progressively increase their access.**

> ***MORE INFO*** **An article posted in the SANS Institute InfoSec Reading Room, "A Detailed Analysis of an Advanced Persistent Threat Malware" (*http://www.sans.org/reading_room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware_33814*), provides insight into the multiple techniques used by APTs. Malware delivered in a targeted spear-phishing email to a political figure was undetectable as malicious by 29 out of 44 antivirus engines. When successfully installed, it made significant system modifications, installed three Trojan spies, and began capturing and sending data to a command-and-control server. Of course, this would be only the beginning. Information gathered from the attack would be used to launch additional attacks by the APT.**

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. An attacker is able to enter data into a webpage and install malware on the system. What should have been done to prevent this?
2. What assets should be evaluated when identifying asset values?
3. What is the primary purpose of vulnerability scans?
4. Who can be a target of an APT?

Objective 1.3: Assess effectiveness of access controls

Access controls should limit access to resources to only the people who need those resources. Two important elements of assessing the effectiveness of the controls are examining user entitlement and performing periodic access reviews and audits.

Exam need to know...

- User entitlement
  For example: Which accounts deserve the most attention when considering user entitlement?
- Access review and audit
  For example: How can you verify whether the principle of least privilege is being enforced?

User entitlement

User entitlement refers to the privileges granted to users when their accounts are first created and during the lifetime of the accounts. One of the primary considerations is ensuring that the principle of least privilege is followed. Users should not have access to more privileges than they need to perform their jobs.

Managing changes during the lifetime of the account can be challenging. Often, the process requires users to submit a request that must go through an approval process, and during this time, the user isn't able to complete job requirements. Bypassing the process improves productivity but sacrifices security. In some cases, the request process is so cumbersome that it's rarely followed.

Ideally, all changes are recorded in logs, creating an accurate audit trail. The audit trail can be used during an audit or review to determine whether the approval process is being followed. When someone's account is granted administrative privileges, the audit trail provides information about who requested the change, who approved it, and who implemented it. It can also identify the source of unauthorized changes.

Administrator and other accounts with elevated privileges deserve the most attention when considering user entitlement. This includes controlling the number of users granted privileged access and limiting the number of users who can grant elevated privileges to others.

It's common to require administrators to use two accounts. Administrators log on with a regular account to perform typical day-to-day work; this account has limited privileges. They log on with the administrator account only when they need to perform administrative tasks.

True or false? All accounts deserve the same level of attention when managing user entitlement processes.

Answer: *False*. Administrative and other privileged accounts deserve more attention than regular user accounts. Accounts with privileges can cause the most damage to a company if misused.

EXAM TIP **User entitlement involves more than just assigning privileges when an account is created. It also includes all the changes that occur during the lifetime of an account.**

Access review and audit

Performing routine access reviews and audits helps an organization know whether security policies related to user accounts are being followed. This includes checks related to entitlement, provisioning, usage, and revocation.

One goal is to determine whether least privilege policies are being followed. A simple method is to periodically check the membership of groups that have a high level of privileges. For example, membership in administrative groups should be limited, and a routine audit will detect whether unauthorized individuals have been added.

Another method is reviewing logs that record user access and user provisioning. An organization will often define procedures for granting additional privileges to any user. A review of the logs used to track this process will determine whether the process is being followed or bypassed.

A security policy will typically specify whether accounts should be disabled or deleted for ex-employees, and a review can determine whether the policy is being followed. Cross-checking active accounts with an employee list can identify potential issues.

These checks can also discover unauthorized accounts. Imagine an administrator who is fired for cause but retains administrative access immediately after the exit interview. It takes less than a minute to create an account and give it full administrative privileges, including the ability to access the network from a remote location. Even if the ex-employee's account is disabled, 15 minutes later the damage is done.

A review can also determine whether administrators are using their accounts as dictated by the security policy. For example, administrators are commonly required to use two accounts—one for regular day-to-day work and the other for administrative purposes. Administrators might be tempted to use the administrative account all the time and never use the regular account. A review of the logs can identify whether administrators are using the regular accounts and how often they're using them.

True or false? When performing an access review, access to all data should be examined.

Answer: *False*. Only access to sensitive data should be examined. A review that examines access to all data will be extremely large and include data available to all users.

EXAM TIP **Access reviews and audits should be repeated periodically, such as every six months or annually. Additionally, administrative or IT personnel should not do the review because the review is designed to inspect the processes and procedures of administrative and IT personnel.**

MORE INFO **Symantec published an interesting white paper, "User and Group Entitlement Reporting," which you can access here: *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_entitlement_reporting_01-2006.en-us.pdf*. It provides a good overview of user and group entitlement and includes some insight into what to look for when evaluating entitlement processes.**

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. A user requires elevated privileges to perform a task once a week. What is the best way to assign these privileges?
2. What can be reviewed to determine whether an organization is complying with existing access control policies?

Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

The identity and access provisioning life cycle directly addresses the management of accounts from creation to deletion. When an account is first created, it is provisioned with appropriate privileges. During the useful lifetime of an account, these privileges are often modified and the account needs to be periodically reviewed to ensure that it has not been granted excessive privileges. When the account is no longer being used, such as when an employee leaves the company, it should be disabled as soon as possible and deleted when it has been determined that it is not needed.

Exam need to know...

- Understand issues related to provisioning of an account
  For example: What is permission creep?
- Understand review
  For example: Which accounts are the most important to review during the identity and access provisioning life cycle?
- Understand the importance of revocation
  For example: What should be done to a user account when an employee leaves the company?

EXAM TIP **If you compare the information in the current Candidate Information Bulletin (CIB) with the previous one, you'll see that the "and access provisioning life cycle" is a new topic. Some of the concepts are similar, but it's worthwhile to recognize the importance (ISC)^2 is implying by adding the objective.**

Provisioning

Provisioning refers to creating accounts and granting them access to resources. Role-based access control (or group-based) is often used to simplify management. Accounts are placed into groups that have defined privileges. As a best practice, all privileges are assigned via the role or group, and individual accounts are not granted privileges directly.

Some organizations use software to automate the provisioning process. For example, when an employee is hired, someone from the human resources department might enter the employee's information into an internal website application. This application is tied to a database and can automatically create the account and add it to the appropriate groups based on where the new employee will work.

Provisioning also occurs during the lifetime of an account when additional privileges are needed. For example, a salesperson assigned to the sales department needs privileges assigned to salespeople. If this person transfers to the IT department, the account is modified, adding privileges needed in the IT department.

Permission creep is a common problem that occurs when previously needed privileges are never removed. For example, someone who transferred from the sales department to the IT department no longer needs privileges assigned to salespeople. Without a procedure in place to remove unneeded privileges, many users progressively collect more and more privileges.

The use of roles or groups helps prevent permission creep. Users can be added and removed from the roles based on their current jobs, and they will automatically have the correct privileges.

Password policies and account lockout policies are often considered to be part of provisioning. Passwords are the weakest form of authentication, but strong password policies help ensure that users create strong passwords and regularly change them. They commonly include the following elements:

- **Password length** As tools to crack passwords become better and processor strength increases, the recommended length has also increased. An older recommendation is a password length of eight characters, but many security professionals now suggest a password length of 12 or more characters. Privileged accounts should be 15 or more characters.
- **Complexity** Passwords should have at least three of the four character types (uppercase, lowercase, numbers, and symbols). For the greatest complexity, passwords should include all four character types.
- **History** Users should be prevented from reusing the same password. A password history will often remember the last 12 or 24 passwords used by an account.
- **Maximum age** Users should be required to regularly change their passwords. Privileged accounts might be required to change their passwords every 30 days, and regular users might be required to change their passwords every 45, 60, or 90 days.

- **Minimum age** This setting requires users to wait before they can reset their password again, and it is often set to one day. It prevents users from repeatedly resetting their password to bypass the history requirement and reuse the same password.

Account lockout policies lock out accounts when incorrect passwords are entered too many times. For example, they can be set to lock out an account after the user enters the wrong password five times in a 30-minute period. The account can be set to remain locked until an administrator unlocks it or for a set time such as 15 minutes. Some policies implement a delay after two or more failed login attacks and are very effective at preventing brute force attacks.

Password reset systems reduce costs by allowing users to reset their passwords without administrative intervention. Many require users to answer secret questions during a registration process, and these questions are later used to validate the user's identity before resetting the password. Attackers have used social engineering methods to learn these secrets and impersonate the user during the reset process. Password reset systems that communicate via email are less susceptible to these types of attacks.

True or false? Account de-provisioning is an important process that helps ensure that the principle of least privilege is enforced.

Answer: *True*. Account de-provisioning is the practice of removing privileges that are no longer needed and prevents permission creep.

EXAM TIP **Processes should be in place to manage and audit the provisioning of an account throughout its lifetime. Without clear procedures, users often collect additional privileges and end up with more privileges they need. A review or audit can discover the problem.**

MORE INFO **Microsoft published a collection of technical papers titled Microsoft Identity and Access Management Series, which is available as a free download from here: *http://www.microsoft.com/download/details.aspx?id=17974*. This package includes a wealth of information that is valuable in understanding provisioning in centralized access control and federated identity management systems. The "Provisioning and Workflow" paper provides some excellent information on provisioning, the identity information life cycle, and different methods used to manage the identity life cycle.**

Review

Accounts should be reviewed periodically to ensure that company policies are being followed. Privileged accounts are the most important to monitor so that misuse is quickly detected. It's often possible to detect suspicious activity by reviewing the logged activity of these accounts.

Groups are commonly used to grant privileges, and monitoring membership in these groups is also effective during a review. As a best practice, privileges should be granted only to a group or role rather than to an individual.

Monitoring group membership isn't the only review, though. The privileges assigned to the groups should also be periodically reviewed. Groups are assigned privileges based on job tasks. As additional job responsibilities are added, additional privileges can be added without removing unneeded privileges. Also, it's easy to focus only on permissions during a review, but the rights assigned to subjects should also be reviewed.

True or false? System logging is an effective measure used to identify misuse of privileged accounts.

Answer: *True*. System logs provide accountability as long as effective identification and authentication methods are used.

> ***EXAM TIP*** **Periodic reviews are an important part of identity and access provisioning. They help identify whether security policies are being followed in the provisioning process and can be part of a formal access review and audit.**

Revocation

Revocation of account access is a concept that most people understand, yet it is often not followed in practice. When an employee leaves the company, the account should be disabled as soon as possible. When the account is no longer needed, it should be deleted.

This is especially important for employees who have administrative privileges. There are more than a few stories where administrators were fired but retained access long enough to create unauthorized accounts with full administrative privileges that they later used to launch attacks.

Human resources (HR) departments can be valuable in keeping access control current. They know when employees are changing jobs and permissions should be changed, and they know when employees are being terminated and accounts should be revoked.

True or false? It is not necessary to immediately disable an account when an employee leaves after giving a notice.

Answer: *False*. It is just as important to disable accounts for employees who leave on good terms as it is to disable accounts for employees who have been fired.

> ***EXAM TIP*** **Accounts should be disabled as soon as possible for employees who leave the company. When an employee is terminated for cause, a policy should be in place so that the account is disabled during the exit interview.**

Can you answer these questions?

You can find the answers to these questions at the end of the chapter.

1. When is an account provisioned?
2. What can be used to review the provisioning process to determine whether the security policy is being followed?
3. When should an account be disabled?

Answers

This section contains the answers to the “Can you answer these questions?” sections in this chapter.

Objective 1.1: Control access by applying the following concepts/methodologies/techniques

1. A security policy. It has an overall goal of preventing loss of confidentiality, loss of integrity, and loss of availability of assets considered valuable by the organization.
2. A detective control. It is being used after an incident to discover what occurred. Audit logs can also be used for access reviews and audits, but, in that case, the logs are a preventive control.
3. An access control list (ACL) is directly associated with an object, and it lists subjects that can access it. An access control matrix combines a capability table with an ACL and lists all subjects and objects.
4. Biometric systems with a low crossover error rate (CER) are better than systems with a high CER. The CER identifies where Type 1 errors (false reject rates) are equal to Type 2 errors (false accept rates).
5. Service Assertion Markup Language (SAML) is used in federated identity management systems to share user information for single sign-on (SSO) between organizations in a federation.
6. A database view is a constrained user interface.
7. Audit trails require strong identification and authorization systems in place. If users are not uniquely identified or can easily be impersonated due to weak authorization, the data in the audit trails cannot be trusted.

Objective 1.2: Understand access control attacks

1. Input validation. Buffer overflow attacks are possible when users can enter unexpected data into a system and access normally inaccessible memory spaces. Input validation checks the data before it is used and prevents this type of attack.
2. All assets, including hardware, software, data, systems, and people, should be evaluated to determine their value.

3. The primary purpose of vulnerability scans is to evaluate the effectiveness of security controls in enforcing security policies.
4. Any person or organization can be a target of an APT. APTs are commonly thought to attack only military and government targets, but they have also targeted civilian organizations and individuals.

Objective 1.3: Assess effectiveness of access controls

1. Create a second account for the user and give it elevated privileges. Instruct the user to use this account only when it is necessary to complete the tasks requiring the elevated privileges.
2. A primary method of review includes the use of audit logs and audit trails. Another method is to identify who is assigned elevated privileges, such as by viewing membership in administrative groups.

Objective 1.4: Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)

1. Accounts are provisioned when they are first created and throughout their lifetime. Provisioning occurs each time privileges are added, and de-provisioning is the process of removing privileges that are no longer needed.
2. Logs and audit trails are the primary method of reviewing the provisioning process. This requires the creation and proper management of logs and audit trails.
3. Accounts should be disabled as soon as it's known that they are not needed. When employees leave a company for cause, their account should be disabled during an exit interview.

Index

About the Author

DARRIL GIBSON, Security+, A+, Network+, CASP, SSCP, CISSP, MCT, CTT+, MCSE, MCITP, is founder and CEO of Security, Consulting, and Training, LLC. Darril has written or co-written more than 25 books, including several on security and security certifications. He regularly posts articles on *http://blogs.GetCertifiedGetAhead.com* and can be reached at *darril@GetCertifiedGetAhead.com*.