EXAM CRAM

CISSP®

Fifth Edition


Cram Sheet


Flash Cards


Practice Tests

MICHAEL GREGG

EXAM CRAM

CISSP® Exam Cram

Fifth Edition

Michael Gregg

CISSP® Exam Cram, Fifth Edition

ISBN-13: 978-0-13-741955-5

ISBN-10: 0-13-741955-4

Library of Congress Control Number: 2021907884

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
Donna Mulder

Technical Editor
Dr. Dwayne Hodges

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Page Layout
codeMantra

Credits

Figure	Attribution/Credit Line
Figure 3-2	Screenshot of World's Biggest Data Breaches © 2021 Information is Beautiful
Figure 4-13	Screenshot of The Burp Proxy Attack Tool © 2021 PortSwigger Ltd
Figure 4-21	Screenshot of X.509 Certificate © Google LLC
Figure 5-5	Courtesy of Cisco Systems, Inc.
Figure 5-6	Courtesy of Cisco Systems, Inc.
Figure 5-8	Courtesy of Cisco Systems, Inc.
Figure 5-9	Courtesy of Cisco Systems, Inc.
Figure 5-10	Courtesy of Cisco Systems, Inc.
Figure 5-13	Courtesy of Unified IT Services Pvt Ltd
Figure 6-5	Courtesy of Cisco Systems, Inc.
Figure 6-6	Courtesy of Cisco Systems, Inc.
Figure 7-1	Courtesy of Cisco Systems, Inc.
Figure 7-8	Screenshot of Tejon Crypter © Rdgsoft.net
Figure 7-9	Screenshot of Ransomware © 2016 Malware Removal Guides
Figure 8-2	Courtesy of Cisco Systems, Inc.

Contents at a Glance

Table of Contents

About the Author

Michael Gregg has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISSP, SSCP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, and CGEIT.

In addition to his experience performing security management, audits, and assessments, Gregg has authored or coauthored more than 25 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has testified before the U.S. Congress, his articles have been published on IT websites, and he has been sourced as an industry expert for CBS, ABC, CNN, Fox News, and the *New York Times*. He has created more than 15 security-related courses and training classes for various companies and universities. Although leading, building, and managing security programs is where he spends the bulk of his time, contributing to the written body of IT security knowledge is how Michael believes he can give something back to the community that has given him so much.

About the Technical Reviewer

Dr. Dwayne Hodges is a retired U.S. Army officer and combat Iraq War veteran with over 25 years' experience. He is the founder and owner of Wellspring Services, a service disabled veteran–owned small business, and he is a senior cybersecurity executive with extensive education, training, and experience working in commercial, government, and military agencies. Dr. Hodges is a university professor, consultant, and board member in higher education with over 17 years' experience with teaching, course development, and curriculum design. He holds a doctorate in education and organizational leadership, a master's degree in information systems technologies and management information systems security, a master's degree in public administration, and a bachelor's degree in sociology and criminal justice. He is a graduate of the U.S. Army Signal Communications School: School of Information Technology, U.S. Army Signal Center, and U.S. Army Command and General College. Dr. Hodges holds several industry certifications and certificates, including $(ISC)^2$ CISSP, CCISO, and CEH; CompTIA Information Security+; Certified Network Defense Architect; Information Technology Infrastructure Library (ITIL); and Certified Encryption Specialist. Dr. Hodges has been a featured TEDx speaker, he is a published author, and he has been a featured speaker for the State of Cyber Security discussions. He has testified in front of the National Academy of Sciences on cybersecurity threats. He is also an author, instructor, and course developer for advanced cryptography concepts on Udemy.

Dedication

I dedicate this book to my godson, Alexander Bucio.
May his life be filled with success and happiness. Mucho gusto!

Acknowledgments

I would like to thank the entire Pearson crew, as they have allowed me to maintain this book over 15 years and 5 editions. It's been a great pleasure to help thousands of individuals prepare for and pass the CISSP exam.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@informit.com

Reader Services

CHAPTER 2

Understanding Asset Security

Terms you'll need to understand:

- Confidentiality
- Integrity
- Availability
- Personally identifiable information
- Information lifecycle management (ILM)
- Data retention
- Data classification
- Data destruction
- Data remanence

Techniques you'll need to master:

- Proper methods for destruction of data
- Development of documents that can aid in compliance with local, state, and federal laws
- The implementation of encryption and its use for the protection of data
- How to use data security controls

Introduction

Understanding asset security is a key requirement of a CISSP candidate. Asset security addresses the controls needed to protect data throughout its lifecycle, from the point of creation to the end of its life. Data protection controls must be implemented to ensure that information is adequately protected during each lifecycle phase. This chapter starts by reviewing the basic security principles of confidentiality, integrity, and availability and moves on to data management and governance.

The CISSP exam requires you to understand data security and how information is protected while it is in transit, in storage, and at rest. You must understand that protection of data is much more important today than it was years ago because data is no longer isolated in standalone servers. Today data often resides in the cloud; data can also be found on laptops, in RAID arrays, or even in paper form. Regardless of its storage location, data must have adequate protection and must be properly disposed of at the end of its useful life.

Basic Security Principles

Confidentiality, integrity, and availability (CIA) are the basic building blocks of any good security program. When defining the goals for network, asset, information, and/or information system security, the term *CIA triad* is commonly used to refer to these concepts. Although the abbreviation CIA might not be as intriguing as the U.S. government's spy organization, it is a concept that security professionals must know and understand.

Confidentiality addresses the secrecy and privacy of information and preventing unauthorized persons from viewing sensitive information. A number of controls are used in the real world to protect the confidentiality of information, such as locked doors, armed guards, and fences. Administrative controls that can enhance confidentiality include the use of information classification systems, such as requiring sensitive data be encrypted. For example, news reports have detailed several large-scale breaches in confidentiality as a result of corporations misplacing or losing laptops, data, and even backup media containing customer account, name, and credit information. The simple act of encrypting this data could have prevented or mitigated the damage. Sending information in an encrypted format denies attackers the opportunity to intercept and sniff plaintext information. The Organization for Economic Co-operation and Development (OECD) specifies that personal data should be limited and provides guidelines for ensuring privacy and confidentiality.

Integrity has to do with accuracy of information and offering users a high degree of confidence that the information they are viewing has not been tampered with. The integrity of data must be protected while the data is in storage, at rest, and in transit. It is important to ensure that unauthorized users have not made any changes and authorized users have not made inappropriate changes. Data in storage can be protected through the use of access controls and audit controls. Cryptography and hashing algorithms can enhance this protection. Cryptography tools include programs such as HashTools, HashCheck, and PowerShell. Likewise, integrity in transit can be ensured primarily through the use of these tools in combination with protocols and frameworks such as public key infrastructure (PKI), digital signatures, and asymmetric algorithms.

Availability refers to the need for information and systems to be available when needed. Although many people think of availability only in electronic terms, availability also applies to physical access. If, at 2 a.m., you need access to backup media stored in a facility that allows access only from 8 a.m. to 5 p.m., you have an availability problem. Availability in the world of electronics can manifest in many ways. 24x7 access to a backup facility does little good if there are no updated backups to restore from and the original copies have been encrypted with ransomware.

Keeping backups is a good way to ensure availability. A backup provides a copy of critical information that can be reinstated if data is destroyed or equipment fails. Using failover equipment is another way to ensure availability. Systems such as redundant arrays of independent disks (RAID) and redundant sites (which can be hot, cold, or warm sites) are two other examples. Disaster recovery is tied closely to availability because it's all about getting critical systems up and running quickly.

Which part of the security triad is considered most important? It depends. In different organizations with different priorities, one part might be more important than the other two. For example, your local bank might consider integrity the most important, an organization responsible for data processing might see availability as the primary concern, and an organization such as a healthcare records clearing agency might value confidentiality the most.

Even though this book refers to the triad as CIA, others might refer to it as AIC or as CAIN (where the *N* stands for *nonrepudiation*).

Security management does not stop at CIA. These are but three of the core techniques that apply to asset security. True security requires defense in depth. In reality, many techniques are required to protect the assets of an organization; take a moment to look over Figure 2.1.

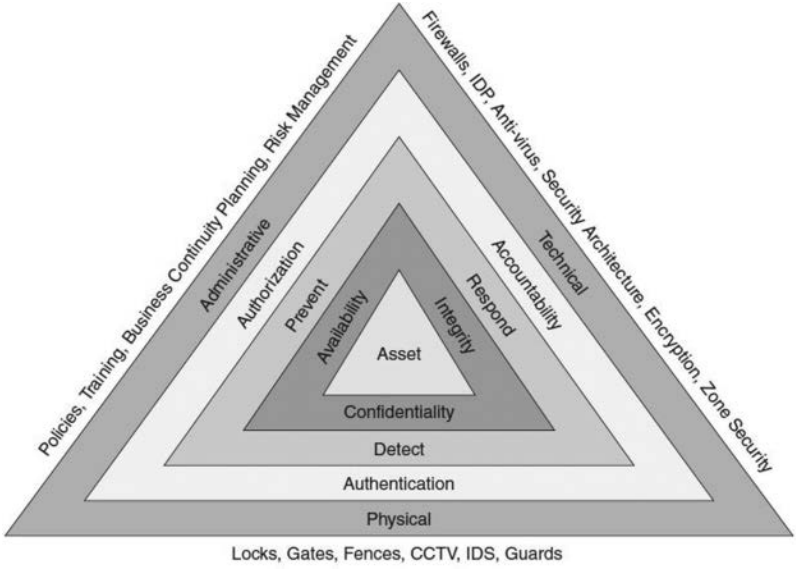

FIGURE 2.1 **Asset Protection Triad**

Data Management: Determining and Maintaining Ownership

Data management is not easy, and it has in fact become more complex recently. Years ago, people only had to be concerned with paper documents, and control might have only meant locking a file cabinet. Today, electronic data might be found on thumb drives, SAN storage arrays, laptop hard drives, mobile devices, and in a public cloud.

Data Governance Policies

Generally, you can think of policies as high-level documents developed by management to transmit the guiding strategy and philosophy of management to employees. A data governance policy is a documented set of specifications for the guarantee of approved management and control of an organization's digital assets and information.

Data governance programs generally address the following types of data:

- Sets of master data
- Metadata

- Sensitive data
- Acquired data

Such specifications can involve directives for business process management (BPM) and enterprise risk planning (ERP), as well as security, data quality, and privacy. The goals of data governance include the following:

- Establish appropriate responsibility for the management of data
- Improve ease of access to data
- Ensure that once data is located, users have enough information about the data to interpret it correctly and consistently
- Improve the security of data, including confidentiality, integrity, and availability

Issues to consider include the following:

- **Cost**: This can include the cost of providing access to the data as well as the cost of protecting it.
- **Ownership**: This includes concerns about who owns the data or who might be a custodian. For example, you might be the custodian of 50 copies of Microsoft Windows Server 2019, yet the code is owned by Microsoft. Users pay for a software license and not ownership of the software itself, and they typically have only the compiled .exe file and not the source code for a program.
- **Liability**: This refers to the financial and legal costs an organization would bear if data were lost, stolen, or hacked.
- **Sensitivity**: This includes issues related to the sensitivity of data that should be protected against unwarranted disclosure (for example, Social Security numbers, date of birth, medical history information).
- **Ensuring law/legal compliance**: This includes items related to legal compliance. For example, you must retain tax records for a minimum number of years, but you might be required to retain personally identifiable information (PII) customer information for only the time it takes to process a single transaction.
- **Process**: This includes methods and tools used to transmit or modify data.

Roles and Responsibilities

Data security requires responsibility. A clear division of roles and responsibility is a tremendous help when dealing with any security issues. Everyone should be subject to the organization's security policy, including employees, management, consultants, and vendors. Specific roles have unique requirements. Some key players and their responsibilities are as follows:

- **Data owner**: Because senior management is ultimately responsible for data and can be held liable if it is compromised, the data owner is usually a member of senior management or the head of that department. The data owner is responsible for setting the security classification of the data. The data owner can delegate some day-to-day responsibility.
- **Data custodian**: The data custodian, who is usually a member of the IT department, does not decide what controls are needed but implements controls on behalf of the data owner. Other responsibilities include handling the day-to-day management of data, controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented.
- **Information security steering committee**: Individuals on this committee are from various levels of management and represent the various departments of the organization. They meet to discuss and make recommendations on security issues.
- **Senior management**: These individuals are ultimately responsible for the security practices of the organization. Senior management might delegate day-to-day responsibility to another party or someone else but cannot delegate overall responsibility for the security of the organization's data.
- **Security advisory group**: These individuals are responsible for reviewing security issues with the chief security officer and are also responsible for reviewing security plans and procedures.
- **Chief security officer**: This individual is responsible for the day-to-day security of the organization and its critical assets.
- **Users**: End users in an organization have responsibilities: They must comply with the requirements laid out in policies and procedures.
- **Developers**: These individuals develop code and applications for the organization. They are responsible for implementing the proper security controls within the programs they develop.

- **Auditor**: This individual is responsible for examining the organization's security procedures and mechanisms. The auditor must provide an independent and objective opinion about the effectiveness of the organization's security controls. How often this process is performed depends on the industry and its related regulations. For example, the healthcare industry in the United States is governed by Health Insurance Portability and Accountability Act (HIPAA) regulations and requires yearly reviews.

ExamAlert

The CISSP exam might test you on the concept that data access does not extend indefinitely. It is not uncommon for an employee to gain more and more access over time while moving to different positions within a company. However, this type of poor management can endanger an organization. When employees are terminated, data access should be withdrawn. If unfriendly termination is known in advance, access should be terminated as soon as possible to reduce the potential for damage.

Data Ownership

Every data object within an organization must have an owner. Any object without a data owner will be left unprotected. The process of assigning a data owner and set of controls to information is known as *information lifecycle management* (*ILM*). ILM is the science of creating and using policies for effective information management. ILM includes every phase of a data object, from its creation to its end. ILM applies to any and all information assets.

ILM is focused on fixed content or static data. While data may not stay in a fixed format throughout its lifecycle, there are times when it is static. For example, after this book has been published, it will stay in a fixed format until the next edition is released.

For the purposes of business records, the lifecycle process includes five phases:

1. Creation and receipt
2. Distribution
3. Use
4. Maintenance
5. Disposition

Data Custodians

Data custodians are responsible for the safe custody, transport, and storage of data and the implementation of business rules. This can include the practice of due care and the implementation of good practices to protect intellectual assets such as patents or trade secrets. Some common responsibilities for a data custodian include the following:

- **Data owner identification**: A data owner must be identified and known for each data set and must be formally appointed. Many times data owners do not know that they are data owners and do not understand the role and its responsibilities. In many organizations the data custodian or IT department by default assumes the role of data owner.
- **Data controls**: Access to data is authorized and managed. Adequate controls must be in place to protect the confidentiality, integrity, and availability of the data. This includes administrative, technical, and physical controls.
- **Change control**: A change control process must be implemented so that change and access can be audited.
- **End-of-life provisions or disposal**: Controls must be in place so that when data is no longer needed or is not accurate, it can be destroyed in an approved method.

Data Documentation and Organization

Organizing and structuring data can help ensure that that it is better understood and interpreted by users. Data documentation should detail the following:

- Data context
- Methodology of data collection
- Data structure and organization
- Validity of data and quality assurance controls
- Data manipulations through data analysis from raw data
- Data confidentiality, access, and integrity controls

Data Warehousing

A *data warehouse* is a database that contains data from many other databases. It allows for trend analysis and marketing decisions through data analytics (discussed later in this chapter). Data warehousing enables a strategic view. Because of the amount of data stored in one location, data warehouses are tempting targets for attackers who can comb through and discover sensitive information.

Data Mining

Data mining is the process of analyzing data to find and understand patterns and relationships about the data (see Figure 2.2). Many things must be in place for data mining to occur, including multiple data sources, access, and warehousing. Data becomes information, information becomes knowledge, and knowledge becomes intelligence through a process called *data analytics*, which is simply examination of data. *Metadata* is best described as being data about data. For example, the number 212 has no meaning by itself. But qualifications can be added to give it meaning; for example, if you learn that 212 is an area code, then you understand that the number represents an area code in Manhattan.

Organizations treasure data and the relationships that can be deduced between individual data elements. These relationships can help companies understand their competitors and the usage patterns of their customers and can help them target their marketing. For example, diapers may be located in the back of the store, near the beer case, because data mining shows that after 10 p.m., more men than women buy diapers, and they tend to buy beer at the same time.

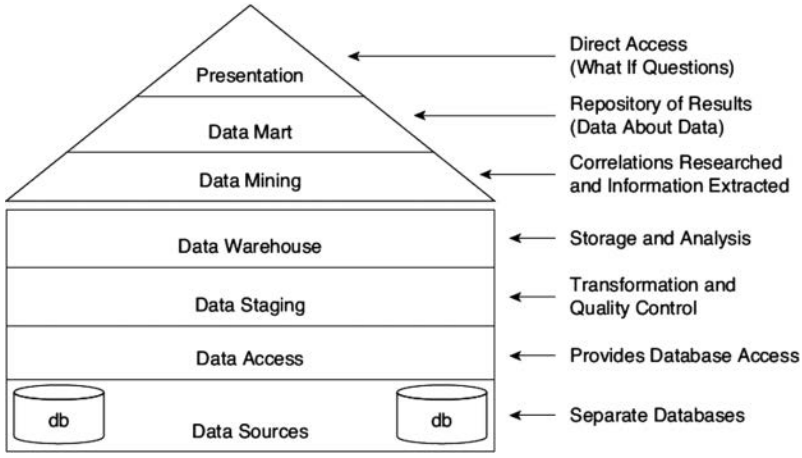

FIGURE 2.2 **Data Mining**

Knowledge Management

Knowledge management seeks to make intelligent use of the data in an organization by applying wisdom to it. This involves turning data into intelligence through analytics by tying together databases, document management, business processes, and information systems. The result is a huge store of data that can be mined to extract knowledge using artificial intelligence techniques.

There are three main approaches to knowledge extraction:

- **Classification**: This approach is used to discover patterns and can be used to reduce large databases to only a few individual records or data marts. (Think of data marts as small slices of data from a data warehouse.)
- **Probabilistic**: This approach is used to permit statistical analysis, often in planning and control systems or in applications that involve uncertainty.
- **Statistical**: This is a number-crunching approach in which rules are constructed to identify generalized patterns in the data.

Data Standards

Data standards provide consistent meaning to data shared among different information systems, programs, and departments throughout a product's lifecycle. Data standards are part of any good enterprise architecture. Data standards make data much easier to use. For example, say that you get a new 850-lumen flashlight that requires two AA batteries. You don't need to worry about what brand of batteries to buy as all AA batteries are manufactured to the same size and voltage standards.

> **Tip**
>
> To see an example of a data standard, check out FDA Resources for Data Standards, at www.fda.gov/industry/fda-resources-data-standards. The FDA provides this site to ensure that common data standards are used throughout the FDA.

Data Lifecycle Control

Data lifecycle control is a policy-based approach to managing the flow of an information system's data throughout its lifecycle from the point of creation to the point at which it is out of date and is destroyed or archived.

Data Audits

After all the tasks discussed so far in this chapter have been performed, the organization's security management practices need to be evaluated periodically. This is accomplished by means of an *audit process*. The audit process can be used to verify that each individual's responsibility is clearly defined. Employees should know their accountability and their assigned duties. Most audits follow a code or set of documentation. For example, financial audits can be performed using the Committee of Sponsoring Organizations of the Treadway Commission (COSO). IT audits typically follow the Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT) framework. COBIT is designed around four domains:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

Although the CISSP exam will not expect you to understand the inner workings of COBIT, you should understand that it is a framework that helps provide governance and assurance. COBIT was designed for performance management and IT management, and it is considered a system of best practices. COBIT was created by the ISACA and the IT Governance Institute (ITGI) in 1992.

Auditors can use COBIT, and this framework is also useful for IT users and managers designing controls and optimizing processes.

Audits make it possible to verify that the controls put in place are working, that the policies that were written are being followed, and that the training provided to employees actually works. To learn more about COBIT, see www.isaca.org/cobit/. Another set of documents that can be used to benchmark the infrastructure is the ISO 27000 family of standards; for details, see www.27000.org.

Data Storage and Archiving

Organizations have a never-ending need for increased storage. Whereas thumb drives were revolutionary and initially provided in the range of 10 MB of storage, today they can provide terabytes of storage. Data storage options in organizations typically include the following:

- Network attached storage (NAS)
- Storage area network (SAN)
- Cloud

Organizations should fully define their security requirements for data storage before deploying a technology. For example, NAS devices are small, easy to use, and can be implemented quickly, but physical security is a real concern, as is implementing strong controls over the data. A SAN can be implemented with much greater security than can a NAS. Cloud-based storage offers yet another option but also presents concerns, including the following:

- Is it a private or public cloud?
- Does it use physical or virtual servers?
- How are the servers provisioned and decommissioned?
- Is the data encrypted and, if so, what kind of encryption is used?
- Where is the data actually stored?
- How is the data transferred (data flow)?
- Where are the encryption keys kept?
- Are there co-tenants?

Keep in mind that storage integration also includes securing virtual environments, services, applications, appliances, and equipment that provide storage.

The Storage Networking Industry Association (SNIA) defines a SAN as "a data storage system consisting of various storage elements, storage devices, computer systems, and/or appliances, plus all the control software, all communicating in efficient harmony over a network." A SAN appears to the client OS as a local disk or volume that is available to be formatted and used locally as needed.

For the CISSP exam, it is important to know the following terms related to SANs:

- **Virtual SAN**: A virtual SAN (VSAN) is a SAN that offers isolation for devices that are physically connected to the same SAN fabric. The use of VSANs is sometimes called *fabric virtualization*. VSANs were developed to support independent virtual fabrics on a single switch. VSANs improve consolidation and simplify management by allowing for more efficient SAN utilization. A VSAN allows a resource on any individual VSAN to be shared by other users on a different VSAN without requiring the SAN fabrics to be merged.
- **Internet Small Computer System Interface (iSCSI)**: iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. Many see it as a replacement for Fibre

Channel because it does not require any special infrastructure and can run over existing IP LAN, MAN, or WAN networks.

- **Fibre Channel over Ethernet (FCoE)**: FCoE, a transport protocol that is similar to iSCSI, can operate at speeds of 10 Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. By contrast, iSCSI is routable because it operates higher up the stack, on top of the TCP and UDP protocols.
- **Host bus adapter (HBA) allocation**: A host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated either through soft zoning or persistent binding. Soft zoning is more permissive, whereas persistent binding decreases address space and increases network complexity.
- **LUN masking**: LUN masking is implemented primarily at the HBA level. It is a system that makes LUNs available to some HBAs but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.
- **Location redundancy**: Location redundancy makes contents accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.
- **Secure storage management and replication**: Secure storage management and replication systems are designed to allow an organization to manage and handle all its data in a secure manner with a focus on the confidentiality, integrity, and availability of the data. A replication service allows the data to be duplicated in real time so that additional fault tolerance is achieved.
- **Multipath solutions**: Enterprise storage multipath solutions reduce the risk of data loss or lack of availability by setting up multiple routes between a server and its drives. The multipath software maintains a listing of all requests, passes them through the best possible path, and reroutes communication if a path fails.
- **SAN snapshots**: SAN snapshot software is typically sold with SAN solutions and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to a physical disk and then make a point-in-time backup copy. Snapshot software is typically fast and makes a copy quickly, regardless of the drive size.

- **Data de-duplication (DDP)**: Data de-duplication is the process of removing redundant data to improve enterprise storage utilization. Redundant data is not copied. It is replaced with a pointer to the one unique copy of the data. Only one instance of redundant data is retained on the enterprise storage medium, such as disk or tape.

Data Security, Protection, Sharing, and Dissemination

Data security involves protecting data from unauthorized activity by authorized users and from access by unauthorized users. Although laws differ depending on which country an organization is operating in, organizations must make the protection of personal information in particular a priority. To understand the importance of data security, consider that according to the Privacy Rights Clearinghouse (www.privacyrights.org), the total number of records containing sensitive personal information accumulated from security breaches in the United States between January 2005 and December 2020 is 11,717,011,063.

The international standard ISO/IEC 17799 covers data security on a global level. ISO 17799 makes clear the fact that all data should have a data owner and data custodian so that it is clear who is responsible for securing and protecting access to that data.

An example of a proprietary international information security standard is the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS sets standards for any entity that handles cardholder information for credit cards, prepaid cards, and POS cards. PCI-DSS comprises 6 control objectives and 12 requirements:

1. Build and maintain a secure network.

   Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2. Protect cardholder data.

   Requirement 3: Protect stored cardholder data.

   Requirement 4: Encrypt transmission of cardholder data across open, public networks.

3. Maintain a vulnerability management program.

   Requirement 5: Use and regularly update antivirus software.

   Requirement 6: Develop and maintain secure systems and applications.

4. Implement strong access control measures.

   Requirement 7: Restrict access to cardholder data based on business need to know.

   Requirement 8: Assign a unique ID to each person with computer access.

   Requirement 9: Restrict physical access to cardholder data.

5. Regularly monitor and test networks.

   Requirement 10: Track and monitor all access to network resources and cardholder data.

   Requirement 11: Regularly test security systems and processes.

6. Maintain an information security policy.

   Requirement 12: Maintain a policy that addresses information security.

Privacy Impact Assessment

Another approach for organizations seeking to improve their protection of personal information is to develop an organization wide policy based on a *privacy impact analysis* (*PIA*). A PIA should determine the risks and effects of collecting, maintaining, and distributing PII in electronic-based systems. The PIA should be used to evaluate privacy risks and ensure that appropriate privacy controls exist. Existing data controls should be examined to verify that accountability is present and that compliance is built in every time new projects or processes are planned to come online. The PIA must include a review of the following items as they adversely affect the CIA of privacy records:

- **Technology**: Any time new systems are added or modifications are made, reviews are needed.
- **Processes**: Business processes change, and even though a company might have a good change policy, the change management system might overlook personal information privacy.
- **People**: Companies change employees and others with whom they do business. Any time business partners, vendors, or service providers change, the impact of the change on privacy needs to be reexamined.

Privacy controls tend to be overlooked for the same reason many security controls are overlooked. Management might have a preconceived idea that security controls will reduce the efficiency or speed of business processes. To overcome such barriers, senior management must make a strong commitment to protection of personal information and demonstrate its support. Risk assessment activities aid in the process by informing stakeholders of the actual costs related to the loss of personal information of clients and customers. These costs can include fines, lawsuits, lost customers, reputation, and, ultimately, the viability of the company.

Information Handling Requirements

Organizations handle large amounts of information and should have policies and procedures in place that detail how information is to be stored. You can think of policies as high-level documents and procedures as step-by-step instructions. Many organizations are in industries that are subject to regulatory standards that detail how and how long information must be retained.

One key concern with storage is to ensure that media is appropriately labeled. Media should be labeled so that the data librarian or individual in charge of media management can identify the media owner, when the content was created, the classification level, and when the content is to be destroyed. Figure 2.3 shows an example of appropriate media labeling.

FIGURE 2.3 **Data Labeling**

Note

Unless you're a classic car enthusiast like I am, it might have been a while since you have seen a working in-dash cassette player. Technology changes, and the requirement to be able to read and access old media is something to consider. Stored media—including older options such as cassette tapes, laser discs, Zip drives, and PATA hard drives—must be readable in order to be useful.

Record Retention and Destruction

All data has a lifetime. Eventually data should either be purged, released, or unclassified. Record retention involves maintaining important information as long as it is needed and destroying or declassifying it when it isn't needed.

Some record retention guidelines are legally mandated by governments. For example, companies typically cannot legally delete potential evidence after a lawsuit is filed and must maintain these assets and records until the court case has concluded. In addition, the JFK Records Act was a record retention act put in place to eventually declassify all records dealing with the assassination of President John F. Kennedy and make these records public by 2018.

The steps in creating a record retention policy include the following:

1. Understand the business needs and any existing regulatory requirements.
2. Classify assets or records.
3. Create retention periods and specify data destruction methods.
4. Develop the policy and determine the impact should the policy not be followed.
5. Conduct training, education, and awareness about the policy.
6. Audit the policy and procedures.
7. Review the policy and procedures regularly.
8. Record the implementation and audit results.

ExamAlert

Two key aspects of data retention are categorization and classification. *Categorization* defines the impact should the asset be exposed. *Classification* defines the value. The CISSP exam is likely to test you on your understanding of these terms.

The Problem of Data Disposal

While hard drive size and performance have continued to grow rapidly, most hard drives and thumb drives are still shipped without encryption enabled. This means, for example, that you can take a hard drive from a computer you bought at an auction that will not boot up, plug the drive into another computer, and possibly gain access to the data on the drive. While many of us have used a paper shredder, few have probably ever sanitized a hard drive. Whether your organization is planning to sell old hard drives, give them to charity, or just throw them away, you need to make sure the data on the drives cannot be recovered.

To find out whether organizations are doing a good job of ensuring that their data is unrecoverable, two researchers from MIT bought 158 used hard drives from eBay. Out of these hard drives, 129 drives still functioned, and 69 of these drives contained data that the researchers were able to copy. The data on these drives included personal information, company HR records, medical information, a pharmacy database, and another database containing several thousand credit card numbers.

Data Remanence and Decommissioning

Object reuse must be carefully considered because information may remain on a hard disk or any other type of media. Even when data has been sanitized, there may be some remaining information. *Data remanence* is the residual data that remains after data has been erased from a storage device. *Sanitization* is the process of clearing all identified content such that no data remnants can be recovered. The CISSP exam will expect you to understand the differences between various types of sanitization methods.

Asset disposal must be handled in an approved manner and must be part of the systems development lifecycle. For example, media that has been used to store sensitive or secret information should be physically destroyed. Before systems or data are decommissioned or disposed of, you must understand any existing legal requirements pertaining to records retention. When archiving information, you must consider the method for retrieving the information.

Clearing and purging are two ways to decommission hardware. Zeroization is a type of clearing. Purging is considered a stronger, permanent form of sanitization. Degaussing and drive wiping are types of purging. The details of these methods are as follows:

- **Zeroization**: This process, which is a type of clearing, is usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices, which would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, *zeroization* involves overwriting the data with zeros. Zeroization is defined in ANSI X9.17. Data may be recoverable with this method.

- **Degaussing**: This process is used to permanently destroy the contents of a hard drive or magnetic media. Degaussing involves using a powerful magnet whose field strength penetrates the media and reverses the polarity of the magnetic particles on the tape or hard disk. After media has been degaussed, it cannot be reused. The only method more secure than degaussing is physical destruction.
- **Drive wiping**: This is the act of overwriting all information on a drive. Drive wiping, which is covered in National Institute of Standards and Technology (NIST) 800-88 and U.S. Department of Defense (DoD) 5200.28, allows a drive to be reused. One form of drive wiping (specified in DoD 5200.28) is overwriting a drive with a special digital pattern through seven passes.

It is common for a storage device to have some remaining amount of information left on it after it has been erased. If the media is going to be reused rather than destroyed, the best practice is to overwrite it with a minimum of seven passes of random ones and zeros.

For information deemed too sensitive, assets such as hard drives, media, and other storage devices may need to be destroyed rather than reused. Destruction, which is the strongest form of sanitization, can include acid baths and physical destruction. If records that are no longer needed are held on a newer non-magnetic drive, such as a solid-state drive (SSD), Curie temperature may be used to heat the drive to the point where it loses its magnetic properties.

ExamAlert

The CISSP exam will expect you to understand the different ways you can dispose of data. One easy way to memorize this is to think of the phrase "Cow, Pig, Sow," or "CP SOW," which stands for **c**learing **c**an be recovered, **p**urging is **p**ermanent, **s**anitizing is the **s**ame, **o**verwriting **o**'s, and **w**iping is **w**riting.

Classifying Information and Supporting Asset Classification

Asset classification involves assigning assets to groups, based on a number of common characteristics. Before you can classify assets, however, you must know what you have. You determine this through an asset inventory. Modern organizations rely heavily on asset inventories and the use of tools such as Asset

Panda, AssetCloud, and ManagerPlus. These applications (and others) assist organizations in identifying, locating, and classifying their assets. The components of an asset inventory include items such as the following:

- Asset name
- Asset location
- Asset cost
- Asset owner
- Asset classification
- Data protection level required

The standard or process used to classify and manage assets is typically left to the discretion of an individual organization. Two things to consider are the size and structure of the organization and what is considered common in the country or industry in which the organization operates. Regardless of the particular approach, the asset classification process consists of five steps:

1. Create an asset inventory.
2. Assign ownership.
3. Classify based on value.
4. Protect based on classification.
5. Assess and review.

> **Note**
>
> To memorize the asset classification process for the CISSP exam, think of CACPA, which rhymes with "Cat Paw" and refers to the steps listed above.

In addition to protecting its assets, an organization must protect the information maintained in those assets that is proprietary or confidential. Data classification is a useful way to rank an organization's informational assets. A well-planned data classification system makes it easy to store and access data. It also makes it easier for users of data to understand the importance of the data. For example, if an organization has a clean desk policy and mandates that company documents, memos, and electronic media not be left on desks, it can change people's attitudes about the value of that information. However, whatever data classification system is used, it should be simple enough that all employees can understand it and execute it properly.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y - Z