10 Security Domains (2011 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: This update supersedes the February 2004 and the February 2010 practice briefs "The 10 Security Domains."

Today's environment requires that HIM professionals understand basic computer security principles to fully protect the privacy of information. The connection between privacy and security is critical for securing electronic health records.

This practice brief outlines the International Information Systems Security Certification Consortium's 10 security domains and highlights the key concepts. The domains provide the foundation of security principles and practices. It is important to note that the 10 security domains are different from the HIPAA security rule.

The Security Domains

Information security must support the mission of the organization. Organizations need to protect their information assets and must decide the level of risk they are willing to accept when determining the cost of security controls.

According to the National Institute of Standards and Technology (NIST), "Security should be appropriate and proportionate to the value of and degree of reliance on the computer system and to the severity, probability and extent of potential harm. Requirements for security will vary depending on the particular organization and computer system."[1]

To provide a common body of knowledge and define terms for information security professionals, the International Information Systems Security Certification Consortium (ISC2) created 10 security domains. The following domains provide the foundation for security practices and principles in all industries, not just healthcare:

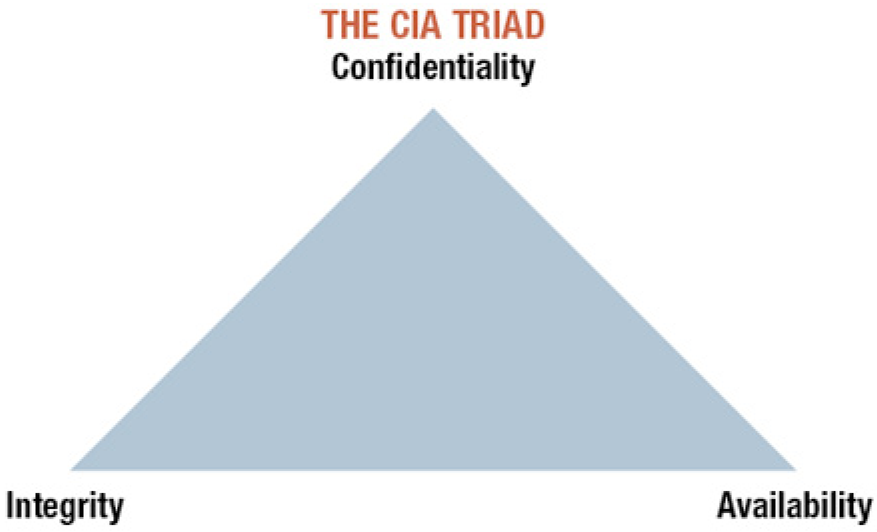
- Security management practices
- Access control systems and methodology
- Telecommunications and networking security
- Cryptography
- Security architecture and models
- Operations security
- Application and systems development security
- Physical security
- Business continuity and disaster recovery planning
- Laws, investigation, and ethics

Security Management Practices

The security management practices domain is the foundation for security professionals' work and identifies key security concepts, controls, and definitions. NIST defines computer security as the "protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (this includes hardware, software, firmware, information/data, and telecommunications)."[2]

NIST outlines three tenets for which security practices should be measured: confidentiality, integrity, and availability. The figure "Confidentiality, Integrity, and Availability (CIA) Triad," below, outlines these three tenets.

Confidentiality, Integrity, and Availability (CIA) Triad



Confidentiality: A requirement that private or confidential information not be disclosed to unauthorized individuals.

Integrity: Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: A requirement intended to ensure that systems work promptly and service is not denied to authorized users.

Source: National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

A key step in security management is risk analysis; that is, identifying threats and vulnerabilities against security controls and measures. A risk analysis allows an organization to estimate potential loss. It also can help determine the most appropriate and cost-effective security measures to implement.

Once the risk analysis is performed, organizations should implement risk management efforts to keep risks at an acceptable level as determined by executive management.

The security management practices domain includes an information classification, such as the unclassified, sensitive, confidential, and top secret classifications used by the United States federal government. Many healthcare organizations use a simpler approach by having only two information classifications: public and confidential. The process of classifying or categorizing information assists an organization by identifying critical information. It provides a foundation for access controls (e.g., need to know) and helps differentiate the types of security safeguards and controls needed to protect each information classification. For example, confidential information requires more protective controls than public information.

Classifying information also identifies roles (such as owner or user), disclosure and distribution, and other criteria such as value, age, useful life, and association.

The final two components of security management are documentation and awareness. Organizations must maintain policies, procedures, guidelines, and standards that direct its documentation efforts. In turn employees must be aware of the organization's security policies and practices. They must recognize the importance of security efforts and understand their role in keeping information secure.

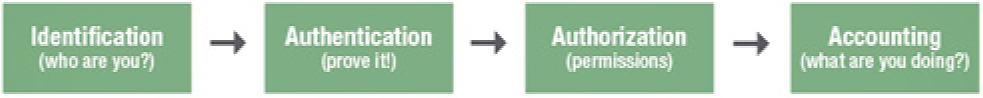
Access Control

In order to maintain information confidentiality, integrity, and availability, it is important to control access to information. Access controls prevent unauthorized users from retrieving, using, or altering information. They are determined by an organization's risks, threats, and vulnerabilities.

Appropriate access controls are categorized in three ways: preventive, detective, or corrective. Preventive controls try to stop harmful events from occurring, while detective controls identify if a harmful event has occurred. Corrective controls are used after a harmful event to restore the system.

"Access Control Process," below, illustrates the primary steps in the access control process.

Access Control Process



Identification is the assignment of unique user IDs. Most organizations base a user's identification off of a person's name; for example, a user ID could be the first letter of a person's first name combined with their last name.

Authentication is the process of proving a user's identity before entering a system. The three primary ways to authenticate users are based upon:

1. Something a user knows (e.g., PIN, password, phrase, pass code)
2. Something a user has (e.g., smart card, ATM card, token)
3. Something a user is (e.g., retina scan, fingerprint, voice scan)

A user's access privileges are based upon some predetermined level of **authorization**, usually established to ensure the user's access is the minimum necessary in order to perform the job. Role-based access is an example of how authorization can be predetermined by management based upon a user's role within the organization.

Physicians generally have the ability to place orders and access more patient information than a nurse who works on a single nursing unit. A volunteer working at the information desk in the main entrance to a hospital is only authorized to access patient census or directory information.

Accounting is the final step in the process. Limiting user access to the minimum necessary can be challenging. Therefore audit controls should be implemented for holding users accountable for their actions.

Source: Harris, Shon. *All-in-One CISSP Exam Guide,* Fifth Edition. Berkeley, CA: McGraw-Hill, 2010.

Telecommunication and Network Security

Telecommunication and network security is one of the most technical of the domains, because it addresses the various structures for a network, methods of communication, formats for transporting data, and measures taken to secure the network and transmission. The key issues of this domain as they relate to each area of the CIA triad are:

Confidentiality

- Network security protocols
- Network authentication services
- Data encryption services

Integrity

- Firewall services
- Communications security management
- Intrusion detection services

Availability

- Fault tolerance for data availability (back-ups, redundant disk systems)
- Acceptable log-ins and operating process performance
- Reliable and interoperable security processes and network security mechanisms[3]

Application and System Development Security

A 2009 report found that more than half of the current cyber attacks are focused on application software vulnerabilities rather than network systems.[4] Special care needs to be taken when developing Web applications that are externally accessed through the Internet. The software code should be written following a secure coding guideline such as the Open Web Application Security Project (OWASP).

Security and privacy professionals must be involved in the software development cycle to ensure that concerns are addressed throughout the process. Information security components should be addressed concurrently in the development cycle (conception, development, implementation, testing, and maintenance).[5]

The following list identifies key security issues at each stage in the development life cycle:

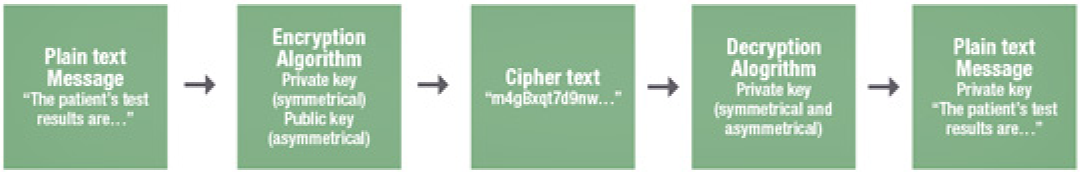
- **System feasibility:** Identify security requirements, including regulatory requirements, internal policies, and standards that will need to be addressed.
- **Software plans and requirements:** Identify the vulnerabilities, threats, and risks. Plan the appropriate level of protection. Complete a cost-benefit analysis.
- **Product design:** Plan for the security specifications in product design (access controls, encryption, etc.).
- **Detailed design:** Balance business needs and legal liabilities within the design of security controls in an application or system.
- **Coding:** Develop the security-related software code and documentation.
- **Integration product:** Test security measures and make refinements.
- **Implementation:** Implement any additional security measures prior to "going live."
- **Operations and maintenance:** Monitor the software and system for changes in security controls. Assess existing controls against newly discovered threats and vulnerabilities. Implement appropriate updates and patches when necessary.

Cryptography

The cryptography domain addresses the security measures used to ensure that information transmitted is readable only by the appropriate individual. In layman's terms, this is commonly referred to as encryption. Encryption is the transformation of plain text into an unreadable cipher text and is the basic technology used to protect the confidentiality and integrity of data.[6]

There are two types of cryptography: symmetrical and asymmetrical. Symmetrical cryptography uses the same private or secret key to encipher and decipher a message. Asymmetrical cryptography uses two different keys: a private key and a public key. For example, the public key can be used to encrypt and send a message and the private key is used to decrypt a message.[7] Confidentiality is maintained because the recipient of the message must use their private key to decrypt the message. "Encryption Process," below, depicts the coding and decoding encryption process.

Encryption Process


Plain text Message
"The patient's test results are..."
Encryption Algorithm
Private key (symmetrical)
Public key (asymmetrical)
Cipher text
"m4gBxqt7d9nw..."
Decryption Alogrithm
Private key (symmetrical and asymmetrical)
Plain text Message
Private key
"The patient's test results are..."

Source: Walsh, Tom. "Selecting and Implementing Security Controls." Seminar. AHIMA and HIMSS, 2003.

While encryption is an addressable implementation specification under HIPAA's security rule, the rules governing breach notification under the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act require encryption methods that render protected health information (PHI) unreadable and meet guidelines established by NIST and the requirements of Federal Information Processing Standards 140-2 to prevent potential breaches. Additionally, vendors of electronic health record systems must be able to meet two meaningful use requirements for encryption: §170.302(u) General encryption and §170.302(v) Encryption when exchanging electronic health information.

Security Architecture and Models

Security professionals must understand the entire information system (configuration, hardware, software) to develop appropriate security architecture. For example, an information system based on a client-server model will have unique security concerns. Desktop PCs could contain sensitive business information and have unique risks, threats, and vulnerabilities. A security professional must understand the issues of this architecture and apply appropriate safeguards.

Information security models are used to organize and formalize security policies by providing a concept and framework. There are three main types of security models:

- Access control: This model, common in healthcare, allows organizations to identify classes of users and the information they are permitted to access.
- Integrity: This type of model not only protects confidentiality, but also works to protect the integrity of information. An integrity model prevents information from being modified by unauthorized users and prevents authorized users from making unauthorized changes.
- Information flow: In this model, information is classified and flows in a specified manner based on security policies and rules.[8]

Operations Security Domain

The operations security domain is concerned with implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities.

There are a number of controls that organizations must consider to secure their operations. This domain addresses issues such as implementing:

- Preventive controls to decrease the threat of unintentional errors or unauthorized users accessing the system and modifying information
- Detective controls that help identify when an error has occurred
- Separation of duties by assigning tasks to different personnel, preventing one person from having total control of the security measures
- Back-ups in case a crash occurs and measures to otherwise restore systems
- Measures for tracking and approval of changes or reconfiguration to the system
- Employee background checks and screening for positions that have access to higher sensitive information or control security measures
- Appropriate retention policies as dictated by organization policies, standards, and legal and business rules
- Appropriate documentation such as organizational security policy and procedures, security, contingency, and disaster recovery plans
- Protections for hardware, software, and information resources

In addition to controls, sound security operations include appropriate monitoring and auditing. There are three types of techniques used to monitor security: intrusion detection, penetration testing, and violation analysis. Auditing is the review of audit trails on a regular basis, which can help alert an organization to inappropriate practices.

Physical Security Domain

The physical security domain addresses the environment surrounding the information system and appropriate countermeasures to physically protect the system.

Physical and environmental threats or vulnerabilities may have been identified using a hazard vulnerability assessment. This includes specific situations such as emergencies, service interruptions, natural disasters, and sabotage.

The environment also must be controlled and concerns addressed around electrical power (noise, brownout, humidity, and static), fire detection and suppression, heating, ventilation, and air conditioning.

Beyond the environment, physical security includes access controls such as locks, guards, surveillance monitors, intrusion detectors, and alarms. It also includes appropriate control of computer equipment by maintaining an inventory system, retention and storage, and destruction process.

Business Continuity Planning and Disaster Recovery Planning

Plans must also be in place to preserve business in the wake of a disaster or disruption of service. This domain addresses two types of planning: business continuity planning and disaster recovery planning. Although the concepts are very similar in nature, there are some differences.

Business continuity planning is the "process of making the plans that will ensure that critical business functions can withstand a variety of emergencies. Disaster recovery planning involves making preparations for a disaster but also addresses the procedures to be followed during and after a loss."[9]

There are four main phases in the business continuity planning process: scope and plan initiation, business impact assessment, business continuity plan development, and plan approval and implementation.

Disaster recovery planning aids the organization in making critical decisions and guiding action in the event of a disaster.

For information security, the plan usually focuses on the data centers or computer rooms that house the servers and network equipment that make up the information technology infrastructure. The plan addresses how these systems would be systematically recovered in the event of a disaster to the data center or computer room.

Law, Investigations, and Ethics

The final domain establishes an expectation that security professionals understand the US and international laws pertaining to information security, the types of computer crimes that can be committed, and the issues unique to investigating a computer crime, such as the appropriate way to gather, control, store, and preserve evidence.

This domain also includes breach notification procedures. The federal government has specifically outlined the procedures that must be followed by covered entities and business associates after a breach of PHI under the HIPAA privacy rule.

Security Credentials

There are several credentials for information security professionals commonly found in healthcare including:

- CISSP-Certified Information Systems Security Professional, credentialed through the International Information Systems Security Certification Consortium
- CHPS-Certified in Healthcare Privacy and Security, credentialed through AHIMA
- CISA-Certified Information Systems Auditor, credentialed through the Information Systems Audit and Control Association

The CISSP credential is based on the 10 security domains addressed in this practice brief; however, it is not specific to healthcare. The CHPS is specific to healthcare and includes most of the security domains outlined in this practice brief and also tests on knowledge of HIPAA's security and privacy rules, including the changes made to privacy and security by the HITECH Act under the American Recovery and Reinvestment Act.

Certified security professionals are morally and legally held to a higher standard of ethical conduct.[10] For example, ISC^2 establishes a code of ethics for credentialed security professionals, which includes four main canons:

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

The 10 security domains are an excellent foundation for understanding security practices, common terminologies, and standards for the profession. HIM professionals should understand the basic tenets of the domains to better communicate and work with information system and security staff.

Notes

1. National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.
2. Kurtz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide (Gold Edition).* Indianapolis, IN: Wiley, 2003, p. 345.
3. Ibid.
4. The SANS Institute. "The Top Cyber Security Risks." September 2009. Available online at www.sans.org/top-cyber-security-risks.
5. National Institute of Standards and Technology. *An Introduction to Computer Security*.
6. Walsh, Tom. "Selecting and Implementing Security Controls." Seminar. AHIMA and HIMSS, 2003.
7. Kurtz and Vines. *The CISSP Prep Guide*, p. 203.
8. Ibid., p. 272.
9. Ibid., p. 379.
10. Ibid., p. 439.

Reference

International Information Systems Security Certification Consortium. "Code of Ethics." Available online at http://www.isc2.org/.

Prepared by

Tom Walsh, CISSP (2009, 2011)

Prepared by (Original)

Michelle Dougherty, MA, RHIA, CHP

Acknowledgments (original)

AHIMA Professional Practice Team
Tom Walsh, CISSP

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA. "10 Security Domains (2011 update)." *Journal of AHIMA* (Updated July 2011).