The 10 Security Domains (AHIMA Practice Brief)

In today's electronic and hybrid environment, HIM professionals must understand computer security concepts to fully protect privacy. Securing an individual's electronic health information is integral to protecting privacy. The connection between privacy and security is critical for HIM professionals to understand. The ability to understand basic security principles is equally as important.

This practice brief will identify the foundation of security—the 10 security domains—and provide a highlight of each domain's key principles. It is important to note that the 10 security domains are different from the HIPAA security rule. These domains provide the foundation of security principles and practices.

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. The best, newest, or costliest technology isn't necessarily the right solution for every organization. "The cost should be proportionate to the value and degree of reliance on the computer system and the severity, probability and extent of potential harm—the requirements for security will vary depending on the particular organization and computer system," according to the National Institute of Standards and Technology (NIST).[1]

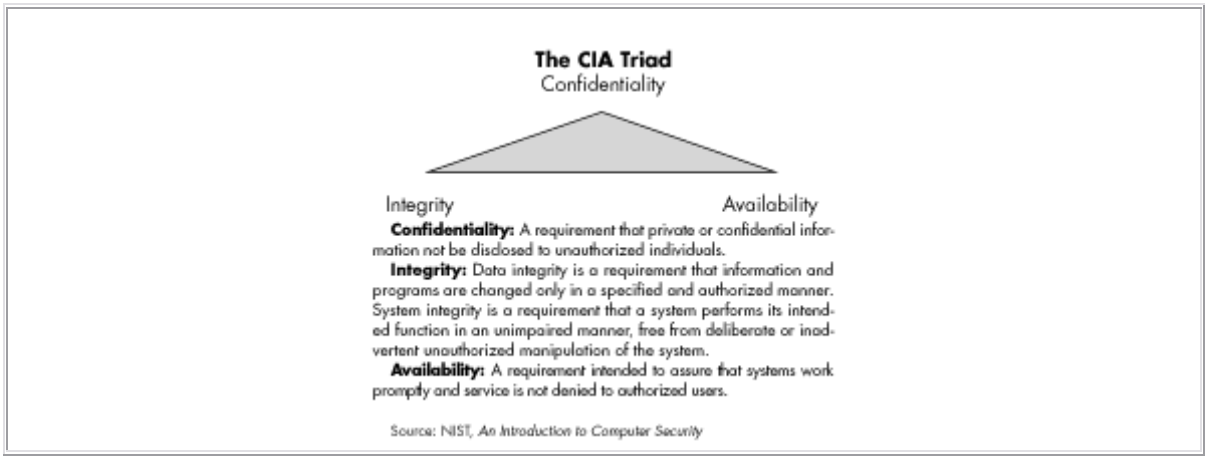
To provide a common body of knowledge and define terms for information security professionals, the International Information Systems Security Certification Consortium (ISC)[2] created ten 10 security domains. These domains provide the foundation for security practices and principles in all industries, not just healthcare:

1. Security management practices
2. Access control systems and methodology
3. Telecommunications and networking security
4. Cryptography
5. Security architecture and models
6. Operations security
7. Application and systems development security
8. Physical security
9. Business continuity and disaster recovery planning
10. Laws, investigation, and ethics

The majority of this practice brief will provide highlights of each security domain for a basic understanding of the concepts. If you are interested in pursing a credential in security, there are resources available with the details needed to fully understand the concepts and principles of each domain.

Security Management Practices

The security management practices domain sets the foundation for security professionals by identifying key 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] The confidentiality, integrity, and availability (CIA) triad provides the three tenets for which security practices are measured.



A key step in security management is risk analysis—identifying threats and vulnerabilities and balancing them against security controls and measures. Through a risk analysis process an organization can estimate potential loss. This value will provide data to determine the most appropriate and cost-effective security measures to implement. Once the risk analysis is performed, risk management efforts are implemented to protect an organization.

The security management practices domain includes the classification of data, such as unclassified, sensitive, confidential, and top secret, etc. The process of classifying data assists an organization by identifying the critical information, provides a foundation for access controls (need to know), and helps differentiating the types of protections needed. Not only does classifying data identify the sensitivity levels, but it also identifies roles (such as owner, user, etc.), 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 efforts. 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 data secure.

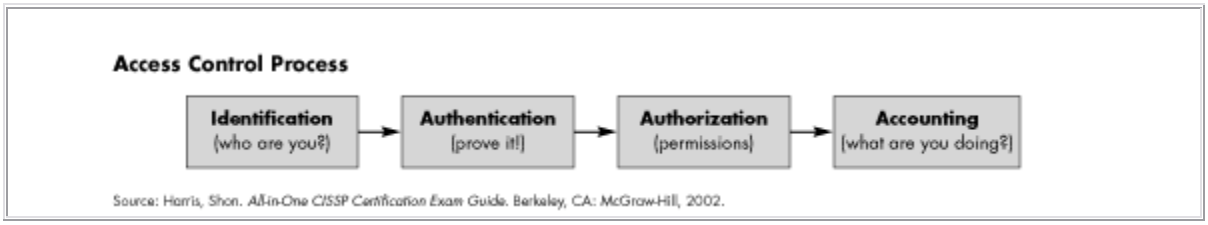
Access Control

In order to maintain confidentiality, integrity and availability of data, it is important to control access to the information system. Controls prevent unauthorized users from accessing the system and/or altering data. They also prevent authorized users from making unauthorized changes to data. When planning the type of access controls necessary, an organization must evaluate its risks, threats, and vulnerabilities.

Controls placed on access are categorized in three ways: preventive, detective, or corrective. Preventive controls try to stop a harmful event from occurring while detective controls identify if a harmful event has occurred. Corrective controls are used after a harmful event to restore the system.
The key to access controls is declaring who you are when before entering a system and having the system verify that you are allowed access. This is known as identification and authentication. There are three way to authenticate users:

1. Something you know (PIN, password, phrase, pass code)
2. Something you have (smart card, ATM card, token)
3. Something you are (retina scan, fingerprint, voice scan)

"Access Control Process," below, shows how the steps of access controls the process: work by identifying and authenticating a user in the system, then authorizing them the user to use or see access an application or data, and finally accounting for what they are doing.



Source: Harris, Shon. *All-in-One CISSP Certification Exam Guide*. Berkeley, CA: McGraw-Hill, 2002.

Telecommunication and Network Security

The telecommunication and network security domain is one of the most technical, as it addresses the various structures for a network, methods of communication, formats for transporting data, and measures taken to secure the network and transmission. Although too technical and detailed to address in this practice brief, the key issues of this domain as they relate to each area of the CIA triad are highlighted in "Elements of Security Related to Telecommunications," below.

Elements of Security Related to Telecommunications

Confidentiality	Integrity	Availability
• Network security protocols • Network authentication services • Data encryption services	• Firewall services • Communications security management • Intrusion detections services	• Fault tolerance for data availability (back ups, redundant disk systems) • Acceptable logins and operating process performance • Reliable and interoperable security processes and network security mechanisms

Source: Kurtz and Vines, *The CISSP Prep Guide, Gold Edition*

Application and System Development Security

Security professionals must be aware of 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

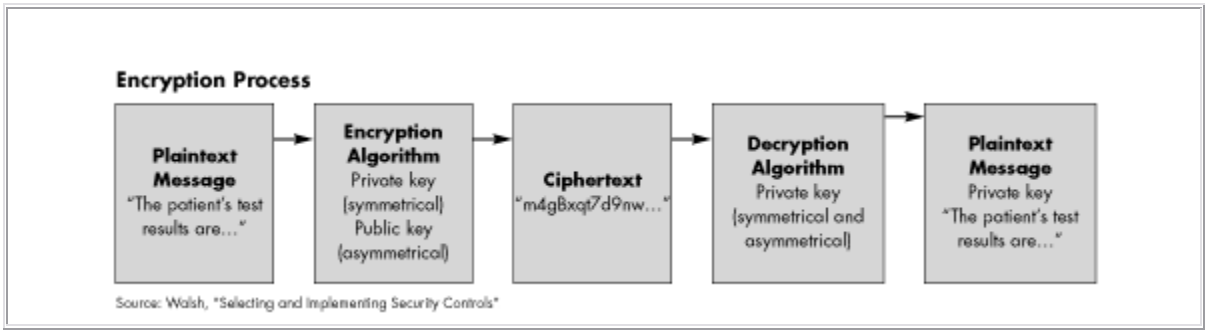
maintenance).[3] The following list identifies key security issues at each stage in the development life cycle:

- **System feasibility:** Identify the security requirements, policies, standards, etc., that will be needed.
- **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:** Design the security controls in relationship to the business needs and legal liabilities.
- **Coding:** Develop the security-related software code and documentation.
- **Integration product:** Test security measures incorporated into software and make refinements.
- **Implementation:** Implement security measures and software and test before "going live."
- **Operations and maintenance:** Monitor security software for changes, test against threats, and implement appropriate changes when necessary.

Cryptography

The cryptography domain addresses the security measures used to ensure that information transmitted is only read and understood by the appropriate individual. In layman's terms, this is commonly referred to as encryption. Encryption is the transformation of plaintext into an unreadable ciphertext and is the basic technology used to protect the confidentiality and integrity of data.[4]

There are two types of cryptography—symmetrical and asymmetrical. Symmetrical cryptography utilizes a private or secret key to encipher and decipher a message. Asymmetrical cryptography uses both a private key and a public key. The public key is used to encrypt and send a message and the private key is used to decrypt a message.[5] "The Encryption Process," below, depicts the coding and decoding encryption process.



Security Architecture and Models

Security professionals must understand the entire information system (configuration, hardware, software, etc.) to develop an 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: [5]

- Access control: This model, common in healthcare, allows organizations to identify users and may classify data to allow or restrict access.
- Integrity: This type of model not only protects confidentiality, but also works to protect the integrity of data. 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.[6]

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 data.
- Detective controls that help identify when an error has occurred.
- A system that provides a separation of duties by assigning tasks to different personnel preventing one person from having total control of the security measures.
- Data backup 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 data or control security measures.
- Appropriate retention policies as dictated by organization policies, standards, legal and business rules.
- Appropriate documentation such as organizational security policy and procedures, security, contingency, and disaster recovery plans.
- Protections for hardware, software, and data resources.

In addition to controls, sound security operations include appropriate auditing and monitoring. There are three types of techniques used to monitor security: intrusion detection, penetration testing, and violation analysis. Another component of monitoring is auditing—performing reviews of audit trails on a regular basis alerts an organization to inappropriate practices.

Physical Security Domain

The physical security domain addresses the environment surrounding the information system and components. The key to this domain is identifying the threats and vulnerabilities and applying appropriate countermeasures to physically protect the system.

All conceivable threats or vulnerabilities should be identified. 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 controls to access such as locks, guards, surveillance monitors, intrusion detectors, and alarms. It also includes maintaining 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 (BCP) and disaster recovery planning (DRP). 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.”[7]

There are four main phases in the business continuity planning process: (1) scope and plan initiation, (2) business impact assessment, (3) business continuity plan development, and (4) plan approval and implementation. A disaster recovery plan aides an organization in making critical decisions and guiding action in the event of a disaster.

Law, Investigations, and Ethics

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

Certified security professionals are morally and legally held to a higher standard of ethical conduct.8 (ISC)2 establishes a code of ethics for credentialed security professionals which includes four main canons:

1. Protect society, the commonweath, and the infrastructure
2. Act honorably, honestly, justly, responsibly, and legally
3. Provide diligent and competent service to principals
4. Advance and protect the profession

Security Credentials

There are three credentials for information security professionals commonly found in healthcare.

- CISSP—Certified Information Systems Security Professional, credentialed through the International Information Systems Security Certifications Consortium
- CHS—Certified in Healthcare Security, credentialed through HIMSS

- CHPS—Certified in Healthcare Privacy and Security, credentialed through AHIMA or HIMSS

The CISSP credential is not specific to healthcare and is based on the 10 security domains addressed in this practice brief. The CHS and CHPS are specific to healthcare. They include principles of the 10 security domains and also test knowledge of the Health Insurance Portability and Accountability Act's security and privacy rules.

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

Prepared by:

Michelle Dougherty, RHIA

Acknowledgements:

AHIMA Professional Practice Team
Tom Walsh, CISSP

Notes

1. *An Introduction to Computer Security*: The NIST Handbook. Washington, DC: National Institute of Standards and Technology, Technology Administration. Washington, DC: U.S. Department of Commerce, 1995, p. 11.
2. Kurtz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide (Gold Edition).* Indianapolis, IN: Wiley, 2003, p. 345.
3. *An Introduction to Computer Security*.
4. Walsh, Tom. "Selecting and Implementing Security Controls." *Getting Practical with Privacy and Security Seminars*, AHIMA and HIMSS, 2003.
5. *The CISSP Prep Guide*, p. 203.
6. *Ibid.*, p. 272.
7. *Ibid.*, p. 379.
8. *Ibid.*, p. 439.

Reference

International Information Systems Security Certifications Consortium, (ISC)2. "Code of Ethics." Available online at www.isc2.org.

Article citation:
Dougherty, Michelle. "The 10 Security Domains" (AHIMA Practice Brief) *Journal of AHIMA* 75, no.2 (February 2004): 56A-D .