The 10 Security Domains (Updated 2013) - Retired

Save to myBoK

Editor's note: This update supersedes the February 2004, February 2010, and May 2012 practice briefs "The 10 Security Domains."

In today's healthcare environment, HIM professionals must understand basic information 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 10 security knowledge domains that individuals with a Certified Information Systems Security Professional (CISSP) credential must possess. The CISSP is offered through the International Information Systems Security Certification Consortium. The knowledge domains for the CISSP credential provide a foundation of security principles and practices in all industries, not just healthcare. It's important to note that the 10 security domains are different from what the HIPAA Security Rule requires. The HIPAA Security Rule was designed to be comprehensive, scalable and technology neutral so that healthcare organizations could meet compliance according to their size, type and need. The 10 security domains are more "best practices" in nature, are not healthcare specific, and explained throughout this practice brief.

The Security Domains

To provide a Common Body of Knowledge (CBK) and define terms for information security professionals, the International Information Systems Security Certification Consortium (ISC2) created the following 10 security domains for the CISSP credential[1]:

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

Access Control

It's important to control access to information so that organizations can maintain the confidentiality, integrity, and availability of that information. Access controls prevent unauthorized users from retrieving, using, or altering information. These controls are determined by an organization's risks, threats, and vulnerabilities.

The "Access Control Process" below illustrates the primary steps in the controlling a user's access to information.

Access Control Process[2]

Identification (i.e., the assignment of a unique user ID) is step one in the Access Control Process. Most organizations derive a user's ID from his or her name. For example, a user ID could be the first letter of a person's first name combined with their last name. However, some organizations may use other methods (e.g., the user's employee number) to avoid conflicts that emerge when two individuals have the same last name and the same first letter of their first name. For example, Tina Smith and Tom Smith would both have the same user name ('tsmith') unless another method is used. Using an employee number, for instance, enables users to keep the same user ID even if their last name changes.

Unique user IDs are necessary for maintaining accountability. When an organization uses generic user IDs (e.g. floor2nurse), there is no easy way to identify who may have accessed the data.

Authentication (i.e., the process of proving a user's identity before he or she is able to enter a system) is step two in the Access Control Process. There are three primary methods to authenticate users. These methods are based on:

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

Authorization (i.e., a user's access privileges in terms of what he or she can or cannot do within an application or system) is step three in the Access Control Process. For example, authorization may restrict one user to data viewing privileges only, while another user may have the authorization to view and change data. Authorization should be based on the minimum necessary access privileges that a user needs to perform his or her job. Role-based access is an example of how management can predetermine authorization based on a user's job function or role within the organization. For example, physicians generally have the ability to place orders and access more patient information than a nurse who works on a single nursing unit or a volunteer working at the information desk who is only authorized to access patient census or directory information.

Accounting (i.e., tracking the actions that the user takes when logged into the system) is the final step in the Access Control Process. Limiting user access to the minimum necessary can be challenging. Therefore, audit controls should be implemented for holding users accountable for their actions. Holding an individual user accountable for his or her actions can be greatly hindered when user IDs are generic or shared by multiple users because it becomes difficult to identify the specific individual who performed the inappropriate action. Audit controls assist in monitoring for unauthorized access by authorized users. Most HIPAA violations occur when authorized users access systems for a non-job-related need. For example, there are cases were healthcare employees misuse their access and view the medical information of a family member, friend, or perhaps even a celebrity.

Telecommunication and Network Security

Telecommunication and network security is one of the most technical domains of the CISSP credential because it requires an understanding of network infrastructure, methods of communication, formats for transporting data, and measures taken to secure the network and transmission. The network is the vital link connecting information resources to users. Thus, this domain focuses on the design and architecture of the network and its components to prevent the disruption of data flow and intrusion.

The key components of this domain are:

Confidentiality

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

Integrity

- Firewall services
- Communications security management
- Intrusion detection services [and intrusion prevention systems]

Availability

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

Information Security Governance and Risk Management

The security management practices domain is the foundation for a security professional's work. This domain identifies key security concepts, controls, and definitions[4]. It also concentrates on many of the nontechnical aspects of information security while also addressing an analysis of technical risks, including:

- Security governance and policy
- Information classification/ownership
- Contractual agreements and procurement processes
- Risk management concepts [risk analysis]
- Personnel security
- Security education, training, and awareness
- Certification and accreditation

Governance provides the framework that guides and directs the information security program. It helps shape standards, policies, procedures, responsibilities, and measures for monitoring the program to support an organization's business objectives. Within healthcare, governance can be separated into two additional components: Information Governance (IG) and Data Governance (DG).

- Information Governance (IG) is the accountability framework that an organization creates to ensure effective and efficient use of information across the enterprise.
- Data Governance (DG) is the policies, processes, and practices that address the accuracy, validity, completeness, timeliness, and integrity of data (i.e., data quality). Data governance is normally the responsibility of the business unit that uses the data.

Information classification identifies the sensitivity and criticality of information that an organization uses. For example, the U.S. federal government uses information classifications such as unclassified, sensitive, confidential, and top secret. Many healthcare organizations employ a simpler approach in which only two classifications (i.e., public and confidential) are used. Data "owners" determine the safeguards and controls that are necessary to protect this information, and they accept the residual risks associated with an application or system in which the data resides. Classifying information also identifies roles (i.e., data owner or user), disclosure and distribution, and other criteria (e.g., the value, age, useful life, and association of the data). Application or System Owners ("owners") are the individuals that are ultimately accountable for the access to, and use of, information resources that directly support their business operations. Owners usually are at a Director level or higher. For example, the Director of Laboratory is the data owner of the laboratory information system (LIS).

Contractual agreements require business partners that have access to the organization's applications, systems, or information/data to establish similar safeguards and controls. The most appropriate time to obtain commitment to security is during the procurement process. Forcing compliance with security controls after an agreement is signed is not always possible. In the healthcare environment, a business associate agreement should incorporate this information.

Risk management is a process that includes the identification, prioritization, and management of technical and non-technical risk to the confidentiality, integrity, or availability of information. This process can occur after an organization identifies a risk via an assessment, or it can occur when an organization conducts a proactive detailed risk analysis on applications and systems. Risks cannot be eliminated; they must be managed appropriately. A key step in security management is risk analysis (i.e., identifying threats and vulnerabilities against security controls and measures). A risk analysis allows an organization to estimate potential loss. It also helps to determine the most appropriate and cost-effective security measures to implement. After the risk analysis is performed, organizations should implement the safeguards and controls needed to keep risks at an acceptable level as determined by executive management or the data owner.

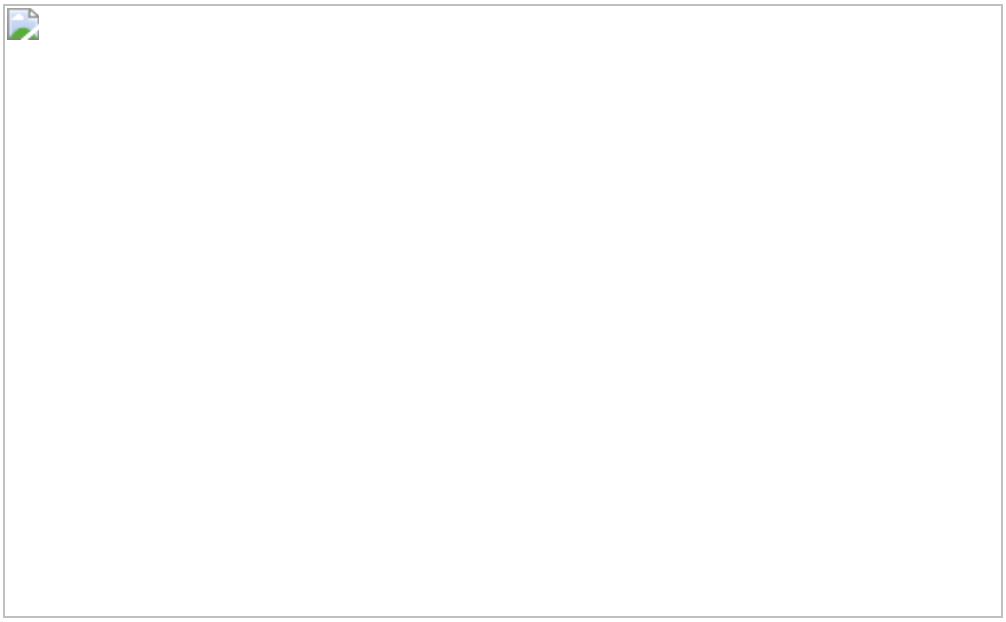
Personnel security is a process during which individuals who have access to the organization's applications, systems, or information/data are screened and managed. , Access to data must be based on the individual's job responsibilities. Organizations must document the entire personnel security process.

Security education, training, and awareness are critical to ensure that workforce members perform their duties in accordance with regulatory requirements. Workforce members must be aware of the organization's security policies and practices. Organizations can accomplish this through security education, training, and awareness. Workforce members must recognize the importance of security efforts and understand their role in keeping information private and secure.

Certification and accreditation is a process during which applications and systems are evaluated and certified in terms of meeting the organization's policies and standards for security control. This is accomplished through a 'seal of approval' system certification and accreditation to attest that applications and systems are secure. Organizations can perform system certification either internally using a certification standard or by an outside firm for an independent validation of system security.

The three primary tenets for information security governance and risk management are: confidentiality, integrity, and availability (CIA). The "CIA Triad" below outlines these three tenets.

CIA Triad



As defined by the National Institute of Standards and Technology[5], the definitions for CIA are:

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.

Software Development Security

The software development security domain focuses on the systems development life cycle (SDLC) from system conception through its design, development, deployment, operation, and eventual retirement from service. Information security and privacy professionals must be involved in all phases of SDLC to ensure the overall effectiveness of security controls and that privacy concerns are addressed.

The proliferation of personally-owned mobile devices (e.g, smartphones, tablets, and laptops) as well as the wide variety of vulnerable mobile apps creates a higher risk of exposing confidential and business-related information in the workplace. This can occur when such information is stored on personally-owned devices. Cyber-attacks often exploit the vulnerabilities inherent in applications and operating systems. That is why frequent updates and patches to software are necessary.

Additionally, special care must be taken when developing internal 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[6].

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 must be addressed.
- **Software plans and requirements:** Identify the vulnerabilities, threats, and risks to software. Plan the appropriate level of protection. Complete a cost-benefit analysis.
- **Product design:** Plan for the security specifications in product design (e.g., access controls or encryption).
- **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 go-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. Ensure the overall effectiveness of application and system security.
- **Product retirement:** Ensure that information that was processed and stored is either retained (i.e., archived), transferred to another database or system, or sanitized (i.e., erased) from the system.

Cryptography

The cryptography domain concentrates on the methods of disguising information to ensure the integrity, confidentiality, and authenticity of information that is transmitted (i.e., data in transit) as well as information that is stored (i.e., data at rest). Cryptography ensures that both types of data are readable only by the appropriate, authorized individual. In layman's terms, this is commonly referred to as encryption. Encryption is the transformation of plain text into an unreadable cipher text.

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 his or her private key to decrypt the message.

"Encryption Process" below is a simple depiction of the coding and decoding encryption process using a private key and a public key.

Encryption Process[7]


Encryption Process

The domain also covers digital signatures and alternatives for rendering information unreadable or unrecognizable to those who do not have a business need to know.

Although 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 provide a safe harbor for data breaches when encryption technology has been utilized. HITECH requires encryption methods that render protected health information (PHI) unreadable. These methods must meet guidelines established by the National Institute of Standards and Technology (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 stage 1 requirements for encryption: §170.302(u) General encryption and §170.302(v) Encryption when exchanging electronic health information. Stage 2 Meaningful Use also incorporates the following core objective and measure which apply to all eligible providers and critical access hospitals:

> Objective:
>
> Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.
>
> Measure:
>
> Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), **including addressing the encryption/security of data at rest** in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

Security Architecture and Design

Each type of information system platform (e.g., workstations, servers, storage area network, switches, firewalls, routers, virtualization, or cloud computing) that makes up the information technology infrastructure has its own unique vulnerabilities.

Security architecture is fundamental to enforcing security policies that can be applied at different layers for each type of system platform. This architecture is based on how the enterprise will handle each of the following:

- Allowable and disallowable services and protocols
- Vulnerability scanning
- Patch management
- Firmware or software upgrades

A security professional then sets standards for safeguards and controls for each platform. When designing the security architecture, a security architect or engineer should take the stance of an attacker to eliminate major vulnerabilities or reduce risks at each of the various platforms. This would entail a network engineer or security professional to use the same methods and tools that a hacker might use to determine vulnerabilities.

Security professionals must have a solid understanding of each type of information system platform to develop appropriate security architecture. The level of protection provided to information systems will vary based on the type of system and the identified risks. Security models are often used to provide a framework for countermeasures to threats and to formalize security policies for access, integrity, and data flow control.

Operations Security

Although the security architect or engineer helps set security standards and policies, operations security is the actual process for implementing, maintaining, and monitoring safeguards and controls on a daily basis to prevent security incidents. Organizations can use numerous safeguards and controls to secure their operations, 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 the event of a crash or measures to otherwise restore systems
- Measures for tracking and approval of changes or reconfiguration to the system (Note: This is typically addressed in a formal change control process and through configuration management that includes an updated inventory of hardware, operating system, and software versions and patches)
- Employee background checks and screening for positions that have access to more highly 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. Three common techniques used to monitor security include:

- **Intrusion prevention/detection:** A process to monitor network traffic or host audit logs for such security violations as intrusions that have gone around or passed through the firewall or intrusions occurring within the local area network behind the firewall.
- **Vulnerability scanning/penetration testing:** An active test run on systems or devices connected to a network to check the current configurations of systems against publicly known vulnerabilities and gauging the level of exposure and determining the overall effectiveness of the current controls.
- **Violation analysis:** An active monitoring program or tool that allows organization to identify areas of trouble. For example, a user repetitively forgets to log out of a clinical application and the application automatically logs the user off after a predetermined period of inactivity. This mistake (time out instead of log off) generates an error message or audit log entry. The analysis of the logs can indicate the need for user awareness reminders to log off when they are finished using a system.

Auditing is the review of audit trails on a regular basis, which can help alert an organization to inappropriate practices.

Business Continuity and Disaster Recovery Planning

Plans must also be in place to preserve and continue business in the wake of a disaster or disruption of service. This domain emphasizes 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. In a healthcare environment, this includes how the necessary information to provide patient care is available. Disaster recovery planning involves making preparations for a disaster but also covers the procedures to be followed during and after a loss."[8]

There are four main phases in the business continuity planning process: 1) scope and plan initiation, 2) business impact analysis which, in healthcare, should include the impact to patient care, 3) business continuity plan development, and 4) 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 disaster recovery plan usually focuses on the data centers or computer rooms that house the servers and network equipment that comprise the information technology infrastructure. The plan details how these systems would be systematically recovered in the event of a disaster to the data center or computer room.

Conduct an exercise to test the plan after it has been developed. The exercise should use a predetermined scenario, similar to a fire or disaster drill. The exercise should evaluate the effectiveness of the plan and the ability of the workforce to follow and execute the plan. An exercise also gives the workforce hands-on training. The results of the exercise will generally reveal where improvements are needed in the plan and workforce training. A documented tabletop exercise (scenario and results) is evidence that the plan has been evaluated.

Legal, Regulations, Investigations and Compliance

Security professionals need to understand U.S. and international laws, regulations, and industry requirements pertaining to information security. This includes cybercrimes and the issues unique to investigating computer crimes, such as the forensic procedures used to gather evidence and the legal protocols for the control, storage, and preservation of the evidence.

This domain also includes breach notification procedures. For healthcare entities and their business associates, the federal government has specifically outlined the procedures that must be followed after a breach of PHI under the HIPAA privacy rule and the HITECH breach notification requirements.

Physical (Environment) Security

The final domain addresses the physical security (i.e., the workplace environment and appropriate countermeasures used to physically protect information assets). Physical and environmental threats or vulnerabilities may have already been identified using a hazard vulnerability assessment. This includes specific situations, such as emergencies, service interruptions, natural disasters, and sabotage.

Physical security includes access controls such as locks, guards, surveillance monitors, intrusion detectors, and alarms. It also includes appropriate control of computer equipment via a maintenance and inventory system, retention and storage, and a destruction process.

The physical environment must protect electrical power (e.g., in the event of noise, brownout, humidity, and static). The environment must also include fire detection and suppression systems as well as heating, ventilation, and air conditioning.

Security Credentials

In addition to the CISSP credential, there are several information security professional credentials that are applicable in the healthcare setting. These include:

- CHPS—Certified in Healthcare Privacy and Security, credentialed through AHIMA
- CISM—Certified Information Systems Manager, credentialed through the Information System Audit and Control Association
- CISA—Certified Information Systems Auditor, credentialed through the Information Systems Audit and Control Association

The CISSP credential is based on the 10 security domains at the core of this practice brief; however, the credential isn't specific to healthcare, and the exam can be difficult to pass because of the depth of technical knowledge needed. The CHPS is specific to healthcare and includes most of the security domains outlined in this practice brief. The CHPS exam also tests one's knowledge of HIPAA's security and privacy rules, including the changes made to privacy and security by the HITECH Act and the Omnibus Rule. This is an excellent certification for individuals who want to expand or demonstrate their

knowledge of healthcare privacy and security. The CISM credential focuses on four domains: information security governance, information security risk management and compliance, information security program development and management, and information security incident management. This credential is helpful for individuals who want to focus more on managerial roles and less on the technical aspects of information security. The CISA credential is focused on the knowledge and skills needed for doing auditing and information security compliance validation.

Certified security professionals are morally and legally held to a higher standard of ethical conduct.[9] For example, ISC2 establishes a code of ethics for credentialed security professionals that includes these 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 members.

Notes

1. The International Information Systems Security Certification Consortium, Inc., (ISC)². Available online at https://www.isc2.org/cissp-domains/default.aspx.
2. Harris, Shon. *All-in-One CISSP Exam Guide,* Fifth Edition. Berkeley, CA: McGraw-Hill, 2010.
3. Kurtz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide (Gold Edition).* Indianapolis, IN: Wiley, 2003, p. 85.
4. The International Information Systems Security Certification Consortium, Inc., (ISC)², Certification Programs, CISSP Domains. Available online at https://www.isc2.org/cissp-domains/default.aspx.
5. National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995, p. 6-7. Available online at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.
6. The Open Web Application Security Project (OWASP). Available online at https://www.owasp.org.
7. Walsh, Tom. "Selecting and Implementing Security Controls." AHIMA and HIMSS seminar, 2003.
8. National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. Available at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.
9. The International Information Systems Security Certification Consortium, Inc., (ISC)², "Code of Ethics" for CISSP. Available online at https://www.isc2.org/ethics/default.aspx?terms=code%20of%20ethics.

Prepared by

Tom Walsh, CISSP (2009, 2011, 2013)

Assisted by

William Miaoulis, CISA, CISM (2011, 2013)

Acknowledgments

Katherine Andersen, RHIT, CCS, CCAT, CPAT
Ben Burton, JD, MBA, RHIA, CHP, CHC
Kathy Downing, MA, RHIA, CHPS, PMP
Elisa R. Gorton, RHIA, CHPS, MAHSM
Lesley Kadlec, MA, RHIA
Michelle Kruse, MBA, RHIA, CHPS
Nancy Prade, MBA, RHIA, CHPS

Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Diana Warner, MS, RHIA, CHPS, FAHIMA

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:
AHIMAAHIMA. "The 10 Security Domains (Updated 2013)." *Journal of AHIMA* 84, no.10 (October 2013): expanded web version.
