

Treadstone 71 Certification

- *HIPAA* requirements: the need for procedural documentation.
- *CISSP* capabilities: multiple methods of securing information.

Training

- *HIPAA* requirements: providing proper training to create a safe and secure environment for the transmission of information.
- *CISSP* capabilities: ability to develop guidelines, standards and procedures to support policies; identification of risks, threats and vulnerabilities; creating security awareness for employees; using risk management practices appropriate for specific resources.

Access Control

- *HIPAA* requirements: the need for access authorization rules for transactions, terminal access, applications, data processes or other users; the need to establish access policies that determine the initial right of access; the need for access modification rules that determine the reasons for modification.
- *CISSP* capabilities: providing access control concepts and methodologies and their enterprise-wide implementation in both centralized and decentralized environments; access control detective and corrective technologies used to minimize or avoid risks, exposures and vulnerabilities; mechanisms for directing or restraining influence over the behavior, use and content of the system to ensure availability, confidentiality and integrity.

Security Occurrence Procedures and Management Process

- *HIPAA* requirements: use of methods to identify security incidents and reporting.
- *CISSP* capabilities: ability to apply laws to computer crimes; how to determine the occurrence of a computer crime; methods of gathering and preserving evidence and investigating crimes.

Media Controls and Physical Security

- *HIPAA* requirements: procedures required to protect information being added to or removed from the system.
- *CISSP* capabilities: providing awareness of threats, vulnerabilities and countermeasures related to physically protecting the enterprise's sensitive information assets.

Security Program Responsibility and Physical Security

- *HIPAA* requirements: assigning an individual to be responsible for security and privacy.
- *CISSP* capabilities: providing awareness of threats, vulnerabilities and countermeasures related to physically protecting the enterprise's sensitive information assets.

Secure Workstation and Physical Security

- *HIPAA* requirements: physical security of workstations.
- *CISSP* capabilities: providing awareness of threats, vulnerabilities and countermeasures related to physically protecting the enterprise's sensitive information assets.

Contingency Planning

- *HIPAA* requirements: tested and accepted plans for disaster recovery and backup of information.
- *CISSP* capabilities: business continuity planning (business impact analysis, resumption strategies) and disaster recovery planning (information systems plan development, implementation and system restoration).

T71, HIPAA and the CISSP CBK

Security Configuration Management Security

- *HIPAA* requirements: a full understanding of hardware and software installations and their implications for security measures.
- *CISSP* capabilities: complete understanding of security models in terms of confidentiality, information flow and commercial vs. government requirements; Internet security services in terms of IETF IPsec; technical platforms in terms of hardware, firmware and software; system security techniques in terms of preventive, detective and corrective controls.

Digital Signatures

- *HIPAA* requirements: need to include message integrity, user authentication and non-repudiation.
- *CISSP* capabilities: full knowledge of basic concepts of cryptography; public and private key algorithms in terms of their applications and uses; algorithm types, key distribution and management and attack methods; the application, construction and use of digital signatures to provide authenticity of electronic transactions and non-repudiation of messages.

Communication and Network Controls

- *HIPAA* requirements: organizations that use the network for communication of data should be aware of security issues surrounding transmission of information; ensuring that information is not accessible by others outside the organization (e.g., use of encryption).
- *CISSP* capabilities: knowledge of communications and network security as it relates to voice, data, multimedia and facsimile transmissions; Internet/intranet/extranet networks in terms of firewalls, routers, gateways and various protocols; communication security management and techniques which prevent, detect and correct errors so that integrity, availability, and confidentiality of transactions over networks may be maintained.

Security Relationship Management Safeguards for Data Authentication

- *HIPAA* requirements: data integrity and authentication guidelines and security concepts for software, hardware and network.
- *CISSP* capabilities: security concepts used to ensure data and software integrity, confidentiality and availability; the security and controls that should be included within systems and application software; the steps and security controls in the software life cycle and change control process.

Audit Controls, Personnel Security and Authorized Use

- *HIPAA* requirements: ability to track access, changes in information and security issues; proper authorization is necessary to access information.
- *CISSP* capabilities: the resources must be protected; the privileges must be restricted; the control mechanisms available; knowledge of the potential for abuse of access; the appropriate controls; the principles of good practices.

It is evident by these comparisons that the certified security practitioner can be extremely beneficial in ensuring *HIPAA* compliance in a healthcare organization, as well as provide *HIPAA*-level processes to any organization. In these times of heightened security awareness, that can be a significant factor in protecting an organization's critical information infrastructure.