ISC2

Domain 1 Key Takeaways

Overall, security professionals reviewing CISSP Domain 1 must develop a comprehensive understanding of the principles, concepts, and best practices related to information security management. This includes not only technical skills but also an understanding of legal and regulatory requirements, risk management, and security governance.

1. Security governance is the foundation for effective information security management. Security policies, standards, and procedures must be established and maintained to guide the implementation of security controls and ensure that resources are allocated appropriately.

2. Risk management is critical to the success of any information security program. The process involves identifying, assessing, and mitigating risks, as well as selecting and implementing appropriate security controls to manage those risks.

3. Security controls are the technical and administrative measures used to protect information and systems from unauthorized access, disclosure, or destruction. Technology professionals should be familiar with the different types of security controls and know how to select and implement them appropriately.

4. Compliance with legal and regulatory requirements is essential for organizations operating in any industry. Technology professionals need to be familiar with the relevant laws and regulations and understand how to comply with them.

5. Core security principles, such as confidentiality, integrity, and availability, are the foundation of information security. Technology professionals must understand how these principles apply to different types of information and systems and know how to implement security controls to protect them.

ISC2

Ethics

Ethics, like everything else, must be included in policies and procedures, and the ethics committee must vigilantly review and monitor. You, as a security professional, are there to set an example. What you see and do will, in fact, become the new practice.

ISC2 Code of Ethics

All information security professionals who are certified by ISC2 recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all ISC2 members are required to commit to fully support this Code of Ethics (the "Code"). ISC2 members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. ISC2 members are obligated to follow the ethics complaint procedure upon observing any action by an ISC2 member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

There are four mandatory canons in the Code. Such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
- *Act honorably, honestly, justly, responsibly, and legally.*
- *Provide diligent and competent service to principals.*
- *Advance and protect the profession.*

Security Concepts

- Information that is not kept secure can lead to actions that cause unintended, unwanted, and possibly illegal death, injury, or damage to property.

- Maintaining confidentiality, integrity, and availability of assets is the basic goal of information security.

- The confidentiality, integrity, and availability (CIA) triad as an information systems security model is popular, largely for its simplicity. It is essential that authenticity, non-repudiation, safety, and privacy are also included in larger scale thought models of information systems security practices.

Security Governance

- Efficiency, safety, and security come with making processes reliable and repeatable; organizational governance is the overarching process (or meta process) that links achieving these efficiencies to the organization's goals and objectives.

- Security functions within an organization to reduce potential impacts on the organization's assets, its people, and its attainment of goals and objectives. Security governance that does not align properly with organizational goals can lead to implementation of security policies and decisions that unnecessarily inhibit productivity, impose undue costs, and hinder strategic intent.

- An organization's hierarchy is often determined by the goals of the organization or the industry it operates in. This structure can impact how security governance is created and implemented, or even how security functions are performed.

- Due care and due diligence have clear legal and financial definitions that carry over into the information systems security profession. These are duties that must be upheld or performed by individuals in any position of authority or responsibility regarding the lives, assets, property, or interests of others or of their own.

- Regardless of whether the organization treats standards as compliance requirements or advisories, in almost all cases the specifics of any given standard need to be carried over into the operational procedures that people will use to perform work (and keep it safe and secure).

Compliance, Legal, and Regulatory Issues

- Maintaining the security posture of an organization is not limited to identifying and handling technical risks. Compliance with internal and external mandates is required to uphold business stability.

Requirements for Investigation Types

- The type of investigation depends on the type of incident, what the organization does with the findings, and whether the organization is under a specific regulation that may require its own investigation. There are four main types of investigations: administrative (internal), civil, regulatory, and criminal.

- There are many industry standards for investigations, including IT security and data investigations; applicable standards for a given organization depend on many variables, such as geographic region/jurisdiction, the nature of the data in question, and the business of the organization.

Develop, Document, and Implement Security

- Despite nonstop changing context, the organization must develop and use various security controls to stay compliant with frameworks and requirements sets. One proven recipe for highly resilient and reliable organizations is to focus attention on their most resilient and adaptable element: people.

Business Continuity (BC) Requirements

- Business continuity is one of the most important things any organization must define to assure the business will survive disruptions of various sources. Building the organizational capacity to respond to and survive major disruptive events requires the organization to grow from surprise intolerant, through tolerating surprises, to being resilient, adaptive, and agile in the face of surprises.

- The BIA is the effort to determine the value of each asset belonging to the organization, as well as the potential risk of losing assets, the threats likely to affect the organization, and the potential for common threats to be realized.

- BCDR is a lengthy and potentially expensive undertaking for businesses, and for this reason, it may be a low priority for some organizations. However, depending on the organization's business sector, it may be a legal requirement, with the healthcare and financial sectors being two obvious examples. Organizations are typically required to determine compliance with applicable mandates. Often, the tools, processes, and activities used to perform compliance reviews are referred to as audits (or auditing). A compliance failure can and will have heavy consequences for an organization.

Contribute to and Enforce Personnel Security

- Personnel policies and procedures can and should address protecting the organization from the fact that people make mistakes or harmful choices, or have malice aforethought, while at the same time cutting through the fog of fear, uncertainty, and doubt about the safety, security, and reliability of the organization's information-based business processes.

- Both internal and external personnel should be required to sign applicable NDAs, AUPs, and in some cases, go through internal training to ensure they are aware of the sensitivity of information and the handling policies every person who accesses the organization's information systems is required to uphold.

Risk Management

- The important takeaway from all risk management frameworks is that risk management should be like breathing: something that is a part of everything we do, throughout the day, year in and year out. Broadly speaking, risk management is a set of Plan–Do–Check–Act (PDCA) cycles spanning all timeframes or decision horizons that any organization faces. In business terms, something is at risk if there are circumstances outside of the organization's control or influence that could cause items to be lost, destroyed, taken away, or otherwise diminished in value or contribution to the organization.

- In an ideal world, the organization has a reasonably complete and up-to-date enumeration or inventory of its information assets. It has also made a set of decisions about how those assets should be valued, in terms of acquisition, replacement, and lost opportunity costs (if the outcomes the assets support are diminished in value by a risk event) or another basis. This valuation is important, since it sets a ceiling for the amount worth investing in mitigating, transferring or avoiding the risk altogether.

- When selecting and implementing security controls, it is always preferable to use multiple types and implement them among the various categories rather than to rely on one type or category; this is called defense in depth (DiD or layered defense), where controls of various types and kinds overlap each other in coverage.

- As with anything an organization does, its risk management processes should be subject to measurement, analysis, and continuous improvement.

- When an organization uses an external provider for managed services, the parties must establish a mutual understanding of exactly what will be provided, under which terms, and at what times. This should include a detailed description of both performance and security functions.

Security Awareness, Education, and Training

- To reduce both the internal threat and the effectiveness of certain types of attacks (e.g., social engineering), it is crucial that the organization teaches employees and staff to recognize security problems and operate in a secure manner. Due care requires effective education, training, and awareness programs for the employees; due diligence requires an evaluation of the effectiveness of that training.