CISSP in 100 Pages:

A Study Companion

By: The Last Minute Exam Cram Team

Foreward:

The field of computer security is an ever-expanding one, with countless job opportunities to appropriately qualified and certified individuals. The purpose of this booklet is not to provide a comprehensive review of the eight domains being assessed on the CISSP. There are other, more complete textbooks for that. It is our hope that this publication will be a helpful supplement to your other study materials. A way to review, and solidify your knowledge. Good luck on your certification exam.

~*The Last Minute Exam Cram Team*

Disclaimer

The information in this book is provided for education and informational purposes only. No warranty or any kind is expressed or implied, including warranty of accuracy, completeness, or fitness for any specific purpose. The information herein is not intended to be and does not constitute financial or legal advice. You understand that you are using any and all information available in this book at your own risk.

Table Of Contents:

Domains

1. Security and Risk Management

2. Asset Security

3. Security Engineering

4. Communication and Network Security

5. Identity and Access Management

6. Security Assessment and Testing

7. Security Operations

8. Software Development Security

Domain No. 1[1]

Security and Risk Management[2]

(Security, Risk, Compliance, Law, Regulations, Business Continuity)

Overview

Security and Risk Management is one of the domains of the CISSP examination. It is concerned with the dissemination of general information related to the Security and Risk Management and covers the basic security principles connected with

- **Confidentiality**
- **Availability**
- **Integrity**

that forms the basis of the security functions.

The candidates are tested for sufficient knowledge in these areas as this forms the basis for the Security Governance and Compliance.

The main focus of testing of CISSP candidates revolves around the general ethical considerations and the ISC Code of Ethics as is the case with all other ISC Examinations. This is to make sure that the candidates exhibit a higher degree of Ethical Code while applying their acquired skills during the CISSP Certification.

For the successful implementation of Information Security Function the security policies and procedures must be applied regularly in a careful manner. Due to this the candidates doing their CISSP certification are tested for their skills necessary for the due development and implementation of the policies within the Information Security Framework.

The candidates doing the CISSP certification must also have enough knowledge in various aspects that make up for the

[1] Watch this video on Domain 1 (1 hr 5 min)

[2] Part Two of Video (2 hrs 11 min)

- Continuity Planning
- Recovery Point Objectives
- Business Impact Analysis
- Requirements Gathering etc.

It is pertinent to note that in the modern Information Security context Risk Management becomes very vital for the overall safety and security of the whole Information System itself. As such the CISSP candidates are thoroughly tested for their proper understanding of the concepts that make up the Risk Management. The following topics in the Risk Management are included in the testing procedure:

- Risk Analysis
- Countermeasures
- Selection and Implementation
- Risk Monitoring
- Reporting
- Risk Frameworks.

In addition to this, proper introduction is given to the Threat Modeling and the proper ways to integrate Risk Management concepts for the risk free acquisition and management of Software, Service Contracts and the Hardware that are using them.

The candidates appearing for the CISSP certification should have good knowledge in the Personnel Security Policies and will be tested for their ability to establish and maintain a high level of prowess in educating, training and conducting programs of awareness in the Risk Management concepts.

The primary areas of knowledge will be

1. Understanding and application of the concepts of Confidentiality Integrity and Availability

These are the three fundamental information security concepts and comprise the C-I-A triad and are considered to be the most important basis of Information Security.

Here you will understand the concepts of Security Governance, classification of data as well as Risk Management, for setting up your Missions, Goals and Objectives. For this you have to practice all relevant policies of security, follow the prescribed standards, and act as per the established standards and procedures to ensure overall security of your system.

You will be required to take stock of the necessary management practices that are put in place for assuring information security. You are also responsible for identifying the security education, conduct required training, create the degree of awareness and utilize the opportunities present for the accomplishment of the concepts of Integrity, Confidentiality and Availability in respect of the Information security.

Under this domain you will be concerned with ensuring confidentiality of data by preventing the unauthorized using of or disclosure of information, and how you will ensure that only authorized persons alone have access to it.
You will be learning how to safeguard the accuracy as well as completeness of the information and methods used for information processing thereby ensuring the highest possible integrity of Information.

You will be also learning how to ensure availability of the information so that only the authorized users have timely and reliable access to the information, assets and associated systems at all times when they need it.

.

2. The Process of Application of Security Governance Principles

Here as a CISSP certified information security specialist you will be able to set the right ways of achieving the goals of the Organization. You will give shape to its Mission statements in a secured and safe environment and help it achieve all the business objectives without losing its credibility, safety and security. Towards this you will be taking stock of all the available business cases, and get hold of the required resources and plan your security functions and set a budget for the same.

As the activities of the organization may involve in many of the activities like acquisitions from both private individuals, or private companies as well as from the Government, it is necessary that as a CISSP professional you will be concerned with ensuring of security of all transactions with that of third parties. This is true for all transactions of sales and disposals by way of divestitures. As a person in charge of security of the organization you will also take care of constituting governance committees and oversee their activities ensuring information and other security while dealing with third parties.

> "THE INFORMATION SECURITY FUNCTION WILL NOT BE VERY SUCCESSFUL WITHOUT CAREFULLY CONSTRUCTED AND UNIFORMLY APPLIED SECURITY POLICIES AND PROCEDURES AND CANDIDATES WILL BE TESTED ON THEIR ABILITY TO DEVELOP AND IMPLEMENT POLICIES AND PROCEDURES WITHIN AN INFORMATION SECURITY CONTEXT." *~CISSP HANDBOOK*

Though everyone in an organization is responsible for the information security, no one is truly accountable. To avoid this and to fix the specific responsibilities on each and every one of the stake holders including employees, vendors, consultants, interns, contractors etc, you will be entrusted with the task of defining specific roles and fastening responsibilities on each one of them.

As a CISSP professional you will be also called upon to assemble necessary control frameworks to help all the stake holders of the Organization to understand their limits and know how to act within their allotted spheres and perform their roles, fulfill their responsibilities without any conflict.

As the security of the information is of paramount importance for the success of the organization you must have mastered all the necessary steps for assuring the information security by exercise of due care in all your activities.

Diligence is the watchword while ensuring information security, and for this you must ensure that all the activities you plan towards the fulfillment of the Confidentiality, integrity and availability of information is carried out in the most diligent way.

The following are the areas of study for your CISSP certification:

- How to align security functions to achieve desired Goals, Mission and Objectives of the business like Business Cases, acquiring necessary resources and planning budget etc.

- Defining the Organizational Processes like Acquisitions, Governance Committees, and Divestitures etc.

- Defining the Roles of Security and the Responsibilities

- Building up of necessary Control Frameworks

- Exercising Due Care

- Exercising Due Diligence

3. The process of Compliance

Compliance with various Legal provisions, Rules and standards are vital for the day to day running of the Organization. Towards this as the man on the spot burdened with the compliance of various Rules and Regulations to maintain the standards of information security you have to be well aware of the compliance requirements.

In addition to this you have to be well prepared to exercise constant monitoring and follow up of various processes and procedures for substantial compliance of Governmental regulations and those that you have set for yourself to maintain the Confidentiality, Availability and Integrity of the information security system.

For complete legal compliance you have to be well versed in the following study areas during your certification as a CISSP:

- Providing for Legislative and Regulatory compliance
- Providing for Privacy requirements compliance

4. Study of Legal and Regulatory issues involved in the Information aspect in a Global business scenario

Today we are all living in a Global village and the business scenario has undergone a complete change. In this changed scenario information security assumes a great significance as like opportunities coming to your organization on a global level your organization has to be prepared to meet the threats also that emerge on a global level.

This calls for putting in place strict information security system in place so that your organization is able to ward off threats that are threatening your confidentiality, availability and integrity even from the other side of the world.

When an organization tends to expand its business activities to far off places of the globe it is likely to meet various changes and challenges in its activities. To tackle these and help your organization proceed with its business objectives in other countries and societies you as a CISSP professional is expected to be always on the lookout for threats to your information security and swiftly respond them in a conclusive manner. This helps your business to retain its momentum in spite of increased level of competition and enhanced level of threat to its safety and security.

During global operations your organization will be dealing with people of different cultures, way of doing business, and differing approach to business and this will bring in many problems in the day to day activities having the potential of severely compromising your information security system.

In these circumstances, it is necessary that you have to act with utmost confidence, dedication and proficiency in protecting the information security that is very vital for the continued success of your organization.

Towards this you will be learning more on the following during your preparation for the Certification.

- Computer crimes

- Licensing and Intellectual Property Rights like Trademark and Copyrights, Management of Digital Rights etc)

- Controls imposed on Imports/ Exports

- Trans- Border Data flow

- Privacy Issues

- Data Breaches

5. Understanding the Professional Ethics

Ethics is the most important trait you as a CISSP certificate holder is expected to have. The concept of professional ethics springs from the set of moral values that dictate you what to do in a given situation to comply with the overall expectations of the society at large and your organization in particular. Credibility in action can only come out of the ethical behavior and it is one of the requirements for maintaining your CISSP Certification.

As ethical values are commonly based on the national interest, rights of the individuals concerned, tradition of the location or the industry, culture, or religion and these ethical values are the ones that tell us what we should do in a given situation.

To maintain high level of professional ethics you must know how to overcome and counter act the

.

- Computer Game Fallacy
- Law-Abiding Citizen Fallacy
- Shatterproof Fallacy:
- Candy-from-a-Baby Fallacy
- Hacker’s Fallacy

Towards this study of the following forms part of your study for your CISSP certification

- Exercising the ISC code of Professional Ethics
- Supporting your Organization’s Code of Ethics

6. Study on developing and implementing the documented Standards, Procedures, Guidelines and Security Policy of your Organization

A CISSP certified professional is in total control of the entire information security system and as such he must be well aware of the policies, procedures, guidelines and standards and the way in which they interact with each other in the real life business situations. It is a part of your job to be abreast of all the differences and relationships that come into play during your work routine and be aware of the different types of policies and their applications.

Never forget that the policies, guidelines, standards and procedures are meant to work together and form the basic blue print of the information security program you are conducting. These are necessary to provide good governance; guidance and decision support and help you establish a legal authority inside the organization.

As these are necessary for making cost-effective and efficient information security systems these must not be overlooked at all. These criteria are the ones that define the nature of governance and help in running the day to day operations and help in taking good decisions.

So, study of these topics is included in the CISSP Study area and you are expected to develop a good working knowledge in developing the necessary policies guidelines, standards and procedures.

7. Understanding the requirements of the Business Continuity.

As an Organization cannot be prepared for all types of eventualities that arise through natural calamities and man- made disasters that impact on its functioning, it must be able to resume its operations without much delay. For this, a good security system must be in place that has the widest scope for business continuity and disaster recovery with minimum cost and time so that the Organization is able to recover from the disaster with the lowest possible damage.

The role played by a CISSP professional in the disaster situation is very vital for the disaster recovery and Business continuity. Hence you have to be well versed in all the concepts that deal with the

- Business Continuity Management
- Various components of business continuity planning
- Defining the best practices for business continuity and disaster management
- Putting in place the best practices for easy and swift recovery
- Process necessary for the development, selection and implementation of solutions for the disaster recovery and business continuity
- Setting up of faster recovery options with the use of redundant technologies
- Setting standards and routines for information back up
- Secure management of offsite facilities
- Specifying the types of tests and drills to be conducted during disaster recovery with particular focus to information security

To achieve this as a student for the CISSP certification you will be studying the following in detail

- Developing and documenting the Project Scope and Plan

- Conducting of Business Impact Analysis

8. Providing for and contributing to the Personnel Security Policies

As a CISSP professional you must be aware of the various employment policies and practices and must have sound knowledge in how these policies can be molded in such a way as to achieve the overall information security objectives. For this it is necessary for you to have thorough understanding of all types of information security roles and the individual responsibilities on an Organizational level.

The background checks and the security clearances must be made an integral part of the employment process. These checks will help the organization to know beforehand the type of the candidates they are considering for recruitment and take on-board only those that have higher level of integrity who can be trusted and made a part of the information security system for uncompromising security set up in the organization.

While recruitment, Reference checks with particular focus on the personal, employment and professional integrity must be made compulsory. A due verification of all the data in the employment applications and resumes must be carried out in a strict manner and any discrepancy must be viewed seriously so that no security problems occur at a later date.

Checks must be conducted on credit records of the probable candidates as well as drug testing must be carried out to know the person under consideration is trustworthy and will add value to the organization.

If necessary special background investigation must be conducted on the FBI and INTERPOL records to make sure that the person to be appointed does not pose any security threat to the organization after he has been appointed.

Apart from this periodic post- employment monitoring and screenings must be built into the security system so that the continued good conduct of the employee is assured as long as he remains on the payroll of the organization.

As a part of the security routine within the Organization, carefully drafted Employment Agreements must be executed both at the time of appointment and at the time of promotion to the sensitive posts within the Organization. These Agreements must include the terms of non- compete, non- disclosure and acceptable user policies.

The hiring and termination procedures of the Organization must be designed in such a way that it offers fair treatment and assures the safety of all its information assets. Likewise while giving the Job descriptions at the time of appointment as well as after appointment must be concise, clear and must be able to clearly define the roles and responsibilities with respect to the security of information.

For achieving all these CISPP certification study focuses more on topics including

- Conducting Employment and candidate screening like Reference Checks, Education Level Verification etc.

- Creating the Agreements and Policies of Employment

- Putting in place the right type of Employment Termination Processes

- Creating the right Vendor, Contractor and Consultant Controls

- Providing for Compliance

- Defining levels of Privacy

9. Understanding and Applying the Risk Management Concepts

Apart from the basic concepts of information security, and security fundamentals, risk management is the most important facet of the CISSP certified professional. You will be learning under this concept the importance of the risk management, quantitative risk assessment, methodologies that are used for assessing the risk, making right calculations of risk. You must also know how to safeguard selection criteria for the assessment of risk and fulfill all the objectives in this respect in a safe and secure way.

You must be able to assess the threat and vulnerability of an asset. You should understand the relationship of the threat, vulnerability and risk for the accurate risk assessment in all cases of natural as well as man mane threats. This helps you to assess the vulnerability of a resource, process, product, or system

You will also understand that the risk management consists of three active components of

- Risk Identification
- Risk Analysis and
- Risk Treatment

The risk identification takes place during the risk assessment phase, and depends on the asset valuation that may be either qualitative with reference to the cost of the asset or qualitative stressing the degree of its importance to the organization.

You will learn that an inaccurate asset valuation will be detrimental to the organization while it will give many benefits when this is done in the right way. This is done by taking into account the Initial and maintenance costs for the asset, its organizational or internal cost and the public or external costs.

Once this is determined, a threat analysis is conducted by defining the actual threat anticipated, its possible consequences on the organization, probable frequency of the threat, chances of both manmade and natural threats occurrence are all calculated for conducting a vulnerability assessment.

The next stage in the Risk management is the risk analysis. Here you will be learning how to run a methodical examination of all the elements of risk management like identification, analysis and control for helping the organization to form an effective risk management strategy. This is done by

1. Identifying the assets that need protection
2. Defining the perceived threats
3. Finding the annualized loss expectancy
4. Creating the right safeguards

by following either a qualitative risk analysis or a quantitative risk analysis.

Based on the risk assessment, now you will be required to bring in the right risk treatment that help you select the right types of safeguards and counter measures to mitigate the perceived threats through risk reduction, risk assignment or transference and risk avoidance as well as risk acceptance. You will also get training in managing risk in a cost effective way by knowing how to do the cost- benefit analysis.

Towards this you will be focusing mainly on the following during your study for the CISSP certification namely:

- Identifying and providing for Threats and Vulnerabilities

- Providing Quantitative, Qualitative and Hybrid Risk Assessment and Analysis
- Providing for the Risk Assignment and Acceptance like System Authorization
- Selection of the right Counter-Measures
- Defining ways of Implementation
- Providing for the preventive, detective and corrective types of
- Conducting Control Assessments
- Providing for Monitoring and measurement
- Conducting Asset Valuation
- Creating Reports
- Providing for Continuous Improvement
- Study of Risk Frameworks

10. Understanding and Applying Of Threat Modeling

A CISSP professional's work centers on the understanding and nature of threats your organization is facing and finding effective ways of counter-acting them, minimizing or altogether removing their impacts on the information security. The threats may be either man- made or natural that has the capability of impacting the operations of the business and the organizational assets in an adverse way.

To help you create a systematic process for identifying these threats and vulnerabilities and bring in suitable counter measures to prevent the adverse effects affecting the assets of the organization you will be learning about

.

- Identification of threats like Adversaries, Employees, Contractors and Trusted Partners

- Knowing how to determine and diagram Potential Attacks like spoofing, social engineering.

- Ability to perform Reduction Analysis

- Knowing the Technologies and the Processes that are necessary for remedying threats like Software Architecture and Operations

11. Integrating Security Risk Considerations into Acquisition Strategy and Practice of the Same

A CISSP certified professional occupies an important position in any organization and he has to play multiple roles to safeguard the integrity and usability of the information security system. He has to be well aware of the risk considerations that are likely to have an impact on the overall functioning of the business. Acquisition of assets and materials for the organization is day to day affair and it needs to be monitored constantly to make sure that none of the threats emerge out of this inevitable activity in the organization.

To know how to frame the right acquisition strategy and implement the risk considerations you will be having the opportunity to study the following topics:

- Study of the Software, Hardware and related Services

- Providing for Third Party Assessment and monitoring like conducting On-Site Assessments, exchange of Documents and Review, Review of Policies and Processes

- Prescribing requirements for Minimum Security

- Finding the right Service Level Requirements

12. Establishing and Managing Information Security Education, Awareness and Training

In any Organization, it is necessary to impart the right type of education and training to create the required levels of awareness in the minds of all those who form part of the Information security program. As a CISSP certified person you have to be aware of the ways of training and education for all those in the Organization and for this you must have sound knowledge of all the tools and objectives necessary for the security education and training.

Most of the times it is an overlooked factor that security awareness is taken for granted and overlooked thus paving way for holes in the overall information security during day to day operations by common users. To avoid this you have to be well aware of the ways of

- Bringing in the support of the senior level management for the awareness programs and training

- Must be able to clearly demonstrate that information security is of paramount importance to the organization

- Must show how the level of security impacts on everyone and their individual job functions

- Must be able to design and conduct the right type of training and education as a training too basic will be simply ignored and one that is too technical will not be understood by those in the Organization

- After the training you must be able to include the security information with the day to day activities of the organization

- Apart from this you must be able to follow up the effectiveness of the security training and education and must take immediate corrective steps whenever needed.

During your study for the CISSP program you will find that an effective security awareness program takes one of the following forms of

- A general awareness program
- A formal training session
- Educating those in the Organization

An awareness program conducted for providing the basic security information making everyone understand its importance is offered as an Indoctrination and orientation programs, presentations by way of lectures, interactive CBT's, video presentations etc, or delivery of printed materials in the form of corporate newsletters, periodic bulletins and security posters

Security training is much more effective than an awareness program as it provides more in- depth information with high focus on a specific security related task or a skill. This is usually given in the form of a

- Class-room training
- On- the job training
- Technical or vendor training
- Qualification programs for Apprentices etc
- Security Education is the best way to provide for deepest level of security training.

This can be structured in such a way that it focuses on the underlying principles of security, explaining its methodologies or laying down concepts involved in the security process.

Towards this the CISSP certification study area focuses more on

- Creating the right levels of Awareness, Training and Education required within the Organization
- Conducting periodic reviews of relevancy of content Periodic reviews for Content Relevancy

[3]

Domain No.2[4]

Asset Security

(Protecting Security of Assets)

Overview

Asset security is the second domain of the CISSP examination. This is mainly concerned with the processes involved in the collection, manipulation and protection of information through the entire lifecycle of the Organization. The classification of information and the assets used with all these form the supporting assets, and you will be required to have a sound knowledge in this area with reference to the information security.

Ownership of information, information systems, the business processes involved form the areas of study as the second domain for your certification.

In the present days, we see that there is an explosion in the ways in which we collect and store data in digital form and this becomes the personal information that must be protected though a well defined information security system. The ability to acquire digital information has also given rise to many concerns including that of the privacy considerations which must be protected making it one of the most vital parts of the asset security domain.

You will be studying the following topics with respect to the individual privacy protection including the concepts that deal with the

- Data Owners
- Data Processors
- Data Remanence
- Limiting Factors Of Data Collection
- Factors That Affect Safe Storage of Collected Data

[3] Listen to streaming podcasts episodes for Domain 1 Here

[4] Watch this series of videos on Domain 2

In this context, while studying collection and storage of digital information you have to study about the data retention also. The concepts that deal with the data retention must be studied with particular emphasis on the organizational, legal and regulatory requirements. Due to this you will be tested on all these topics in your CISSP certification examination.

Due to all this, it becomes necessary for the CISSP candidate to have sufficient knowledge in the data collection and storage functions as he will be responsible for the selection and implementation of the right types of data security controls in the Organization.

You will be studying about the following in detail to have sufficient knowledge in

- Defining and implementation of Baselines
- Tailoring and scoping processes
- Selection of standards
- Use of Cryptography etc

In addition to this, you will be also studying about other data handling requirements like data storage, data destruction and data labeling. As a Certified CISSP professional you will be expected to have the capability to conduct evaluation of data handling requirements and be well versed in developing the right type of policies and procedures for secure acquiring, handling and storage of information.

The knowledge areas prescribed for your CISSP certification under the Asset Domain includes

1. Classification of Information and Supporting Assets (E.G., Sensitivity, Criticality)

Classifying data that is being used in the organization is one of the best ways of controlling access to information and the assets associated with it. As the person responsible for the Information security you need to decide and put in place the right access controls to determine who uses which information. You have to ensure that not every user has access to all information and his access must be limited to the needs, position and purpose of the user.

To achieve this type of information security by limiting access to data, the first thing you have to do is to classify data and put in a set of strict protocols to clearly classify the data and allow access to the required people thus preventing unauthorized access to all. The information classification can be based on many variables governed by various criteria. This is one of the vital functions that is the first step towards putting in place a strong information security set- up for your organization.

As the person who is responsible for the security of information you need to assign strict rules of access to each class of persons so that the accidental or malicious attacks on the Information system are fully prevented.

2. Determine and Maintain Ownership (e.g., Data Owners, System Owners, and Business/Mission Owners)

Determining and maintaining ownership, rights and permissions emanating from it is yet another way to implement a good information security protocol. In any organization you can see a number of owners of information and they will be having various types of user policies for their data and information.

Accepting these and putting in place the effective ways of controlling access through permissions for dealing with the information in which they have to deal and deny the permission for others is the way of handling ownership of data and information. Towards this a CISSP certified information security specialist must be having good knowledge in handling the rights and permissions of data owners, system owners, business owners and the mission owners in separate ways.

This is necessary for providing the right type of information security within the Organization without compromising on the confidentiality, availability and integrity of the Information Security System

3. Protection of Privacy

The information security system you are putting in place for your organization must be capable of protecting the privacy of all those connected with it. This must be so tuned towards preventing the unauthorized use or misuse of information collected from individuals.

The CISSP curriculum expects you to have a sound knowledge on how to

- Collect information from individuals in fair and legal manner
- Make sure that the information so collected is used only for the purpose for which it was collected
- Make the information collection process accurate and relevant at all times
- Make these information available to the individuals who have a legal right and permission to access the same
- Update and make them error- free without compromising on their security
- Safeguard the personal information from unauthorized use
- Assure safety and integrity of the personal information when they have to be transmitted to other places or persons who are not bound by the Information system you are maintaining etc.

All these you have to study with reference to the

- ❖ Protection of personal data of Data owners
- ❖ Protection of personal data in the hands of the Data processors
- ❖ Dealing with data security taking into account the Data Remanence of memory devices
- ❖ Assuring personal data security through personal data Collection limitation

> “THE RAPID EXPANSION IN THE COLLECTION AND STORAGE OF DIGITIZED PERSONAL INFORMATION HAS RESULTED IN A CORRESPONDING INCREASE IN THE IMPORTANCE OF PRIVACY CONSIDERATIONS, AND PRIVACY PROTECTION CONSTITUTES AN IMPORTANT PART OF THE ASSET SECURITY DOMAIN.” *~CISSP HANDBOOK*

4. Ensure Appropriate Retention (E.G., Media, Hardware, Personnel)

To ensure the highest possible information security it is necessary to have a good data retention policy as a part of your Organization’s protocol for the secure retention of information for both operational as well as regulatory compliance. As an Information security specialist after your CISSP certification it is necessary to create a data retention policy that provides for

- Organizing the information in a secure way so that they can be searched and accessed whenever needed

- Deletion and disposal of data in a permanent manner when the data is no longer needed without any chance of retrieval at a later date by any unauthorized person

Apart from operational compliance there are many instances for the Regulatory compliance and the data retention policy framed must also be able to provide data and information to the Governmental and other agencies that are legally entitled to receive data from the organization in a secure manner. The data retention policy must also be able to provide for the deletion and permanent removal of data from data storage media, hardware systems and Personnel files as soon as the statutory compliance period is over.

You have to gather as much knowledge as possible on the concepts of data retention in the modern days. You must also be able to provide for the Information security in the Organization with the right types of data retention policy as a way of enforcing good information security protocols.

5. Determine Data Security Controls (E.G., Data at Rest, Data in Transit)

When the data you want to protect is stored in a file or in a media then it is said to be a data at rest. If the same data is in the process of being transmitted through a network, then it becomes a data in transit. Each one of these types of data needs a different set of standards selection for the information security.

For protecting the data at rest the best way is to adopt the Drive and tape encryption that is good for protecting the data even after there is a physical breach of the security controls.

For effective protection of the sensitive data they must be backed up on offsite media or data servers that are governed and protected by their own information security protocols. The transfer of data must be done in a secure way following the standards you have selected for the data in motion. These must be scrupulously followed while sending the data to your offsite storage through data transfer networks electronically or through physical movement of data in a secure backup media.

Scoping is the process of determining which standards you want to use for your organization information security system and this must be done after due consideration of various factors with utmost adherence to the Information security objectives you have set to achieve.

With the use of the concept of Tailoring you will be able to customize a generally available data security standard, so that it is able to work well and give the best possible protection to your organization's data. The process of Tailoring usually begins with the selection of controls for information security, goes on with scoping to avoid those standards that are not good for your information system, and proceeds further to end with the application of compensating controls.

Yet another way of safeguarding the information security of data in motion is cryptography. This is the process of encrypting the information before transfer and decrypting the same after the transfer so that the content of the communication are made unintelligible for all except the person to whom it is meant for.

This system is widely in use today so the CISSP certified information security professional is expected to have a very thorough knowledge in

- Fundamental concepts of cryptography
- Basic concepts of cryptography
- Basic operation of cryptographic systems
- Common uses and applications of cryptography
- Methods of attacks

You must be able to apply the cryptographic concepts to issues faced in the real world situations and problems faced in protecting the sensitive information of the organization. For this you are expected to have a thorough understanding of the strengths, weaknesses, applications and uses of the cryptograph based information security systems.

The following are the topics covered for the CISSP Certification examination under this chapter

- Defining and implementation of Baselines
- Tailoring and scoping processes
- Selection of standards
- Use of Cryptography etc

6. Establish Handling Requirements (Markings, Labels, Storage, Destruction of Sensitive Information

In any organization there will be need to handle data on a day to day basis by different categories of users. You might have placed the way the sensitive data will be created, accessed, stored and retrieved by these categories of users through your information security system. These form part of the handling requirements of information and you have to plan elaborately and set up the right set of these to satisfy how the information will be handled in a safe and secure manner.

The handling requirements involve in creating the right types of markings and labels, so that the data will be handled according to the set of handling routines that you have put in place through your information security system. Efficient and secure information handling function starts from the data classification where the data are clearly classified according to their significance, criticality, value and life of the information.

The importance and sensitivity of the data will determine its type of classification. Once the set of rules for classifying the information have been clearly defined then you have to create the set of rules for marking and labeling them. This makes it easy to identify the type of document and handle it in the way it is planned to be handled for maintaining its confidentiality, availability and integrity.

The crux of the information security in an organization lies in the way the objects are assigned their labels and how they are handled as per these markings. The labeling and marking of information helps in locating and identifying the data that are sensitive in nature. The process of labeling is done as per the scheme put in place for the organizational data classification.

The most common labels used in the present days are

- Top- secret : the information that is likely to cause grave danger to the organization once it is used by unauthorized persons
- Secret : is the type of information that is likely to cause serious damage to the organization
- Confidential: is the type of information that is likely to cause damage to the organization.

Apart from this there are lot of additional labels that are in use to denote and classify the information and this classification helps the Information Security System to ensure the proper handling of the information.

A CISSP certified Information security Professional must be well aware of the problems associated with the destruction of unneeded data contained in physical media or in the electronic memory devices. It is very important to put in place strict rules and routines before the data goes for deletion both manually and automatically. You must be aware of the different types of memories used in the computer systems and how each of them handles the data deletion process and their data Remanence properties.

This is necessary to prevent the unauthorized declassification of sensitive information after the devices that contained these data were subject to non-invasive data deletion processes. You have to know the data storage and data Remanence characteristics of the following types of memory devices connected with computer based information creation, storage, and handling and deletion functions:

- Random Access Memory (RAM)
- Cache memory
- Read Only Memory (ROM)
- Static Random Access Memory (SRAM)
- Dynamic Random Access Memory (DRAM)
- Programmable Read- only Memory (PROM)
- Erasable Programmable Read- only Memory (EPROM)
- Electrically Erasable Programmable Read- only Memory (E EPROM)
- Flash Memories
- Solid State Drives

The data destruction of information covered under your security program must be cleaned secured, or destroyed fully before disposing the devices and files that contained the data to prevent unauthorized retrieval of sensitive data through object reuse. You must know how to prevent the attacks through various types of object reuses and how to safely and completely remove the data before destroying the media by resorting to

- Overwriting
- Degaussing
- Physical Destruction
- Shredding etc

Thus, you will be expected to have the necessary knowledge in these vital areas of Information security and will be tested for while seeking your CISSP certification. [5]

[5] Listen to these Podcasts on Domain 2

Domain No. 3

Security Engineering[6]

(Engineering and Management of Security)

Overview

Security engineering is the third domain of the CISSP Examination. It covers the second largest number of topics that you have to study for your certification.

Security engineering is the process of building and maintaining the required information systems and related sub-systems for delivering the functionalities that are required to withstand and counteract any threats emanating from

- Malicious attacks
- Human error
- Failure of hardware or software systems
- Caused by natural disasters.

Thus, the security engineering encompasses a wide range of systems that are created for ensuring the confidentiality, integrity and availability in engineering systems for the due creation and integration of security controls, behaviors and capabilities into the information systems and the enterprise level architecture.

The main focus of the CISSP certification examination would be to test the knowledge of the candidates in their ability to build, maintain and manage necessary security process through fail proof engineering architectures based on sound and secure design principles. They are expected to have sound knowledge in all the basic concepts of creating and running security models and develop further design requirements for meeting the organizational security requirements and to draw necessary security policies and implement them using the right type of controls and countermeasures for satisfying those design requirements.

To achieve this as the person who is responsible for the security of information in the organization you are expected to have all the knowledge that is necessary for

[6] Here's a Playlist of Helpful Domain 3 Videos

understanding the limitations of security and the capabilities of those systems you depend on for the level of information security you want to maintain.

You will be also be expected to be on constant look out for ways of assessing the nature and extent of vulnerabilities in your information system set up and the architectures that you are using to maintain such counter measures for mitigating the effects of those vulnerabilities and safeguard the safety and security of information.

You have to acquire enough knowledge about the designs and solution elements for creating the right type of engineering architectures that help you tide away all types of threats to the information security and the CISSP examination is designed to test your capabilities and knowledge in the level of preparation to prevent any type of attacks that are targeted to jeopardize the level of security you have to build for the information and data of the organization.

You have to be well versed in the following topics including

- Vulnerabilities on the client and server side
- Security of databases
- Cloud security and distributed systems
- Systems based on cryptography
- Industrial control systems
- Vulnerabilities arising out of web applications
- Vulnerabilities inherent in mobile devises
- Risks and threats arising out of embedded systems etc

You must have a good working knowledge in the concepts of cryptography that helps in the protection of information while it is in motion and also when it is at rest, by suitably altering its readability and usability by unauthorized persons. Cryptography has advanced much in the present times and you must have good knowledge of creating, running and managing cryptography based solutions and systems to ensure the confidentiality, integrity and availability of information. These concepts are well covered under this security engineering domain.

In this respect the candidates of CISSP certification will be tested for their prowess in the

- General cryptographic concepts
- Lifecycle of a cryptography based solution
- System that is necessary for successful cryptography
- Public key infrastructure
- Key practices for creating and managing a cryptography process and system
- Concepts of digital signatures
- Effective Digital rights management

A CISSP student must also possess enough knowledge and good understanding of various cryptanalytic attack vectors like

- Brute force attacks
- Attacks through social engineering
- cipher- text only attacks
- Known plaintext attacks
- Frequency analysis of attacks
- Cipher text and implementation attacks

The branch of study comprising of the security engineering not only covers the information systems development but also the additional topics that cover all the concepts and principles
of creating applications for design of secure information systems with particular reference to the site selection and protection, design of secure facilities and enforcing the required level of physical security.

Areas of Knowledge

1. **Implement and manage engineering processes using secure design principles**

To achieve complete information security it is now possible to use many of the available engineering processes. The aim of using these to the information system is to make them more secure and withstand and counteract the perceived vulnerabilities and threats without causing any damage to the overall information security system.

For this you have to take care of the following namely

- Capture the interactions and relations between the system and the environment in which it is acting
- Formulate the necessary security systems for the system
- Implement the security requirements into the information system

Being a CISSP professional you have to be well aware of the problems associated with the launch and patch approach to overall information security. Due to the use of the distributed information systems in the organization there is a possibility of increasing risks associated with security breaches at all the levels.

> "[CANDIDATES] MUST UNDERSTAND THE FUNDAMENTAL CONCEPTS OF SECURITY MODELS AND BE CAPABLE OF DEVELOPING DESIGN REQUIREMENTS BASED ON ORGANIZATION REQUIREMENTS AND SECURITY POLICIES AND OF SELECTING CONTROLS AND COUNTERMEASURES THAT SATISFY THOSE DESIGN REQUIREMENTS."
>
> *~CISSP HANDBOOK*

So, as the person in charge of information security you have to get the things in the right order from the start and this must be the focus of any security systems design.

But under practical conditions there is always a possibility for the presence of flaws in the system and these are capable of putting the information at risk. You have to know how to manage risks even after you have designed a good system using the best of the engineering processes. So, you must always try to build a system that is good from the start and is able to handle the vulnerabilities arising due to failing components or unexpected events.

While designing your system based on engineering processes for information security you have to bear in mind the importance of

- Seamless matching of the knowledge of the system and its environment
- Mutual trust between the system owner and different users of the system

- Engineering requirements needed to design, create and implement the system
- Modeling of the system based on the latest design principles
- Methods and tools necessary to create and run the system
- How the designed system will be ready to meet the risk management criteria

2. **Understand the fundamental concepts of security models**
   (e.g., Confidentiality, Integrity, and Multi-level Models)

Within an organization there are numerous places where the computer and information security are at play. So, you must be aware of each one of the vulnerability prevailing within the system, and put in place the right type of counter measures to ensure complete information security. For this you must have sound understanding of the security levels of each and every component built into your information security system and provide for the vulnerabilities and threats that each one of them has to face.

A CISSP professional must be able to prepare a blue print for the overall security of his entire information system and for this he can make use of the available or perceived security models that aptly apply to his type of security system. Then he has to take care to implement the blueprint and create the right type of system architecture with the available engineering models so that they are able to withstand and counter act all types of threat to the information security.

Towards this the main focus and testing during CISSP certification will be towards the following concepts of computer based security systems:

- Computer architecture and the individual components that form part of it
- Building and managing trusting computing bases
- Creating effective security mechanisms based on the computer architecture
- Components that form the operating system and their in- built security elements
- Security models that help you create your information security blue print

- Criteria on which your security system is to be operated and ratings for the same
- Conducting the right certification and accreditation processes to make the various users aware of the security aspects of your information security system

3. Select controls and countermeasures based upon systems security evaluation Models

When designing an information security system for your organization it is necessary to take into account various controls and counter measures that will be good to protect the information in all eventualities. As the main aim of good information security system is for ensuring the confidentiality, integrity and availability of data, you have to take care to select one of the best systems security evaluation models available.

In these circumstances, you have to be well versed with the available systems security evaluation models that have all the necessary controls and counter measures built into it. This will help you use the same for creating the elements that make up a secure information system for the organization. The evaluation of the security model you have chosen has to be carried out in a careful manner so that it is able to fulfill all the requirements of your intended information security system.

.

4. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)

All information systems have a set of security capabilities. These must be thoroughly studied so that it is possible to tweak the system in such a way it is made highly secure to protect the information of the organization. You must be well aware of the various factors that affect the security capability of the overall system and must be able to make necessary corrections and changes to the same to get a fully functional and error-free information system for your organization.

For this it is necessary to know the process of memory protection, as it is a way of controlling memory access rights on the computers and the other computer based devices that make up your information security system. This forms part of the most modern computer architecture and operating systems. This prevents the unauthorized processes accessing the memory of the system so that the integrity of the data is protected to a great extent.

5. Assess and mitigate the vulnerabilities of security architectures, designs, and solution Elements

Vulnerabilities and threats are inherent in any Information system and as a Security person in charge of maintaining the confidentiality, availability and integrity of the system you need to know how to assess the weak spots in your information handling and management system.

For this you must have good knowledge in the security architectures on which your information security system has been built on, and the designs of each of the individual components that make up the system. This will help you easily identify the vulnerable aspects of the system and threats you can expect out of them.

When you are able to do this you can easily put in place the right type of information security elements and counter measures to easily tackle them. This must be done on a continuous basis as the vulnerabilities may arise from new instances and you have to keep on looking for new threats and try to counter them by anticipating their happening and likely frequency of those security problems that are likely to occur in the near future.

The vulnerabilities and threats may arise from the client side usage when new applets and applications are used in the system. This may give rise to new challenges by way of unexpected security issues and other instances of security attacks and you must be able to assess the possible security issues that may arise in the system with the use of these new applications and be ready with the solutions for those problems to save the information security system from any possible attacks.

The problems to the information security system may arise due to server based operations like data flow control issues, and it is necessary to have very strict data usage and data handling routines in the server environment to ensure that no security problem occurs in the data storage, or data handling instances between the server and clients operating within the Information security system.

Database forms the backbone of any Commercial operations of the organization and it is of paramount importance to assure the best possible security for the same. As the database is one of the most critical information wealth of the organization the information security system must be well focused and tuned well to take care of any security problem that may arise due to the interference, aggregation, and data mining or during the data analytics functions during normal operations of the organization.

Particular importance must be laid while going in for data warehousing operations and utmost care must be taken to ensure full security for the data and all vulnerabilities and threats must be tackled on priority. Suitable counter measures must be put in place even before the occurrence of the anticipated threats and well planned back up strategies must be laid for maintaining the integrity and safety of the database.

The following areas of study are suggested for successful preparation for your CISSP certification:

1. Client based (e.g., applets, local caches)
2. Server based (e.g., data flow control)
3. Database security (e.g., inference, aggregation, data mining, data analytics, warehousing)
4. Large scale parallel data systems

5. Distributed systems (e.g., cloud computing, grid computing, peer to peer)
6. Cryptographic systems
7. Industrial control systems (e.g., SCADA)

6. Assess and mitigate vulnerabilities in web -based systems (e.g., XML, OWASP)

In the present days the computers and Internet have become the most basic and inevitable part of any business and their dependability on these has brought in new vulnerabilities and threats to their information. Protecting the information and providing for its security becomes very difficult in the global business scenario, due to explosion of web based attacks and hacking attempts.

So, it becomes necessary for the CISSP certified professional to be rightly equipped to meet these challenges and safeguard the information so that the business of the organization is not compromised in any way.

Towards this, you have to be well versed in the concepts that equip you and be ready to assess the vulnerabilities and threats that arise out of your web-based information creation, management and storage systems. You must be fully aware of the various ways of providing for the confidentiality, Integrity and availability of the information at all times.

7. Assess and mitigate vulnerabilities in mobile systems

Use of mobile hand held devices has brought in a new way of creation, handling and storage of information. With the ever increasing number of users of these devices now it is very important for any business to have separate and dedicated information systems for these users to tap on new opportunities that arise out of the mobile technology explosion.

At the same time this type of information handling processes has brought in many new types of challenges and ways of attacking the conventional information security systems in entirely different manners hitherto unexpected and unheard of in the earlier information security parlance.

So, to safeguard the vital data from attacks that emanate from mobile based systems you must be able to assess the types of vulnerabilities and threats that may arise out of mobile systems. You must be able to successfully tackle the problems that arise from a mobile system to the information security systems you have built for your organization.

8. Assess and mitigate vulnerabilities in embedded devices and cyber physical systems (e.g., network - enabled devices , Internet of things (loT))

Embedded systems have become the driving force for the development of the technology based development in all the spheres of today's business activities. We see that many new computational and networked devices and systems are needed to cope with the demands of the present day businesses and these are becoming more vital for the business success. Due to this we depend more on these embedded and cyber physical systems as ways of achieving our business goals in this fiercely competitive global business scenario.

Use of these systems has brought in a new set of threats and vulnerabilities to the information security systems of an organization, and the CISSP certified information security person must be well aware of the dangers that are lurking on this landscape. He must be able to assess the type, extent and frequency of these potential threats to the information system and must be ready to face them with the right types of counter measures to minimize or completely avoid the dangers arising out of the attacks that may arise out of the use of embedded and cyber physical systems.

9. Apply Cryptography

Cryptology is one of the most important ways of protecting the information security and it is fast becoming the right way to counter the vulnerabilities and threats that are to be anticipated while dealing with data in motion as we all as to the data that is stored on a modern cloud based environment. Most of the modern information security systems use cryptology as an inevitable and indispensable part of their information security systems due to its ability to help the organization to meet its goals of information security.

Cryptology can be used for successfully protecting confidentiality of information when the data transmitted or the storage data systems are compromised, the data in the hands of the unauthorized persons becomes useless as they do not have the necessary key to decrypt the information to cause damage to the information security.

> “CRYPTOGRAPHY INVOLVES THE PROTECTION OF INFORMATION, BOTH WHILE IN MOTION AND AT REST, BY ALTERING THAT INFORMATION TO ENSURE ITS INTEGRITY, CONFIDENTIALITY AND AUTHENTICITY.” *~CISSP HANDBOOK*

The cryptography technology also helps in maintaining the integrity of the information by ensuring a higher degree of accuracy due to the use of various hashing algorithms and message digests. The availability of the information can be ensured through cryptology with the use of various secure ways of authentication like digital signatures, digital certificates, Public Key Infrastructure etc.

To make better use of the modern cryptology for information security of your organization you must be have a good

- Understanding of the concepts of symmetric and asymmetric key systems
- Know what keys are and how to use them effectively for meeting your information security goals
- Knowledge to online information safe with the use of right type of cryptology based tools an systems
- Knowledge about the vulnerabilities and threats that are to anticipated in respect of a cryptology based information security system and the counter measures for the same

For this you have to focus more on these topics while preparing for your CISSP certification:

1. Cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)

2. Cryptographic types (e.g., symmetric, asymmetric, elliptic curves)
3. Public Key Infrastructure (PKI
4. Key management practice
5. Digital signatures
6. Digital Rights Management
7. Non- Repudiation
8. Data integrity through Hashing and Salting
9. Methods of Cryptanalytic Attacks like brute force attacks, cipher- text only, known text etc.

10.Apply Secure Principles to Site and Facility design

Site and facility plays an important role not only in the information security realm but also for the overall safety and security of the infrastructure of the entire organization. So, while selecting your site for the facility creation you must have conducted a complete analysis of the threats to the physical security and plan your site and facility design accordingly.

You must be aware of the various physical and environmental security controls and ensure that there is complete fulfillment of all the physical security concepts and controls that are necessary to protect the site and the facilities.

Some of the things that must be satisfied for good site and facility design include

- Factors likely to interfere with physical security
- Elements that must be considered for good facility planning and design
- Security controls that must be established
- Access controls that must be put in place
- Technical controls necessary for effective overall security
- Environmental and life safety controls necessary
- Implementation and operation of the overall security System

11.Design and Implement Physical Security

Threats and vulnerabilities to physical security arises in many forms like

- Natural disasters
- Emergency situations
- Man- made threats
- Sabotages

All these must be properly analyzed and the anticipated threats to physical security must be identified so that proper counter measures are placed at all places so that no damage due to these affects the survival of the facility at any time. The risk analysis carried out must be comprehensive and suitable damage control strategies must be implemented.

Some of the common threats include:

- Threats arising out of fire
- Water and flooding
- Vibration and movement
- Severe and extreme weather conditions
- Electricity hazards
- Sabotage/terrorism/war/theft/vandalism:
- Equipment failure
- Loss of communications and utilities
- Personnel loss etc.

The focus areas for your CISSP examination under this heading include:

Design and implementation of physical security in respect of

- Wiring closets
- Server Rooms
- Media Storage facilities
- Evidence Storage
- Restricted an Work Area Security (e.g Operations centers)
- Data Centre Security
- Utilities and HVAC considerations
- Water issues (e.g., leakage, flooding)
- Fire prevention, detection and suppression [7]

[7] Listen to these podcasts on Security Operations

Domain No. 4

Communication and Network Security[8]

(Designing and Protecting Network Security)

The communication and Network security domain forms an important part of the CISSP certification process as this is one of the core areas of the information security. Due to this in the present day communication set up using various modes of data transmission, storage and handling you are expected to have a deep understanding of various concepts that make up the Network security and the security of information.

Under this domain you will have a clear understanding of the following important aspects that have a very strong impact on the information security in a networked environment like:

- Network Architecture
- Methods of information transmission
- Types of data transport and handling protocols
- Types and nature of control devices in use for secure data communication

[8] Video playlist on communication and network security

- Various security measures necessary for ensuring confidentiality in communication
- Ways to endure integrity and accuracy of information
- making the information available in a secure manner to every user who is authorized to access it
- Types of security measures for transmission of data over private networks
- The security measures that must be adopted while sending data over public networks

As a candidate for the CISSP exam you have to learn the basics of networking like the network topologies, the process and functioning of IP addressing system, concepts of modern network segmentation, various types of data switching and routing, concepts involved in the process of wireless networking, the OSI and TCP models of communication, TCP/IP protocols and their way of functioning with respect to the present day standards of data transmission over the wide area networks.

> "THE CISSP CANDIDATE IS EXPECTED TO DEMONSTRATE A THOROUGH UNDERSTANDING OF NETWORK FUNDAMENTALS INCLUDING NETWORK TOPOLOGIES, IP ADDRESSING, NETWORK SEGMENTATION, SWITCHING AND ROUTING, WIRELESS NETWORKING, THE OSI AND TCP MODELS AND THE TCP/IP PROTOCOL SUITE."
>
> ~CISSP HANDBOOK

In the present days, there is a widespread use of encryption for ensuring the information security while sending data over secured and unsecured data networks. Due to this you will be tested for your basic understanding of the cryptography processes. Particularly you will be tested for your extent of knowledge in the secure network communication.

This domain also requires you to have a good understanding of various modes of communication and ways of ensuring security over the network and you must have a good understanding of security network devices and their ways of functioning and how these can be used in an effective manner for ensuring the right types of security on the network while sending and receiving critical data.

To maintain high degree of information security, a CISSP professional is tested for his depth of knowledge about various devices and equipments that form part of the communication network like switches, routers, and points of access for the wireless systems. They should have sound knowledge and ability to deploy the right combination of these network control devices for maintaining the required level of confidentiality, availability and integrity of data and information sent and received through the communication network.

Candidates of CISSP certification must also possess enough knowledge in various types of security considerations inherent and come built- in with the devices that form the network security in respect of the media through which the information is transmitted. You must also have sufficient knowledge about

- Network access control
- End point Security
- Content distribution Networks etc

As a CISSP certified Information Security Professional you are expected to have the ability to design and implement necessary data transmission protocols, network elements, control devices, for successful and orderly commissioning and running and managing of communication channels. For this you must be well aware of the methods of using various technologies to enable the network to use applications for efficient and secure handling of all types of information like data, voice, remote access, and multimedia content and sending and receiving data over virtualized networks.

You must have good knowledge about network attack factors and must be able to assess the vulnerability of each device or sub- system based on which the network is functioning and must ensure the security over the entire network by knowing how to design, implement, manage and monitor the necessary counter measures to mitigate all types attacks on the communication network.

Key Areas of Knowledge

1. **Apply secure design principles to network architecture**
   (e.g., IP & non-IP protocols, segmentation)

The entire Network architecture must be created with the primary aim of maintaining the highest possible information security and towards this you have to understand the following principles of design of network security architectures like

- **Compartmentalization or segmentation of resources:** the various components and resources that are used for the creation of the network security architecture have different sensitivities. This difference in their level of activity affects the overall security of your information system. To prevent an adverse effect of one of the less sensitive resources on the entire system you must design your network architecture in a way that resources of different sensitivity are located in a security zone that matches their level of sensitivity

- **Layered protections or defense in depth:** When designing your network architecture you must be able to ensure higher degree of protection to your IT system, by making use of different security layers and must be created so that each one complements the other in action for added security.

- **The design should ensure adequate protection:** While designing your network elements make sure that each and every individual element in the network gets adequate protection that are relevant to their anticipated vulnerabilities and frequency of attacks. These must be totally compliant with all the legal requirements and they must be fully co- operative with other elements present in your network system.

- **The design should be simple and have least privileges:** The users of the security system must be able to use the IT resources for performing their day to day routines with minimum privileges for ensuring easy yet secure availability of the system information.

- **Identify the weakest link in the chain:** you must be aware that the overall security of your network system as good as the security of your weakest link in the chain. Your design must take this into account and take care of the vulnerabilities due to this vital aspect and provide the right and timely counter measures so that the damage to the overall network security is as minimum as possible.

While designing your network Architecture it is necessary to adhere to the most modern network transmission protocols. The IP based network protocols are the widest in use and hence the design you are adopting must adhere to these for seamless operation across various networks.

The Open System Interconnection protocol popularly referred to as the OSI model provides for universal interconnection of all the Network related elements, components and devices, and hence the design you create for your network security must follow these standards for easy connectivity across various platforms and networks. On the other hand the TCP/IP model defines the way of sending and receiving data through the Internet and hence these also need to be followed for easy access to any type of network in an internet based network system.

While trying to create a good network security system, you must not forget the fact that an attack targeting any layer or one of the different layers of the network's common stack can take place at any time. Likewise an attack can target a specific layer and you have to conduct a risk analysis for each of the components in the network and know the vulnerability level of each of them and plan, implement and monitor effective counter measures to prevent any damage to the overall network security system.

You have to focus on the following topics while getting ready for your CISSP certification examination:

- OSI And TCP/IP Models
- IP Networking
- Implications Of Multilayer Protocols (E.G., DNP3)
- Converged Protocols (E.G., Fcoe, MPLS, Voip, Iscsi)
- Software- Defined Networks
- Wireless Networks

- Cryptography Used To Maintain Communication Security

2. Secure Network Components

A network may have been built on many components that work in synchronous manner to transfer data from one point in the network to the other. In the present days, we have to use a variety of Network components to successfully design and run a network. As the person in charge of the security of the network and the information you send through the network, it is your duty to take care of the security issues that are likely to arise with each of the individual network components.

You have to conduct a thorough security analysis of each one of these components like

- Bridges
- Modems
- Switches
- Routers
- Wireless access points
- Mobile devices
- Cabling and cabling components

so that you are able to understand the vulnerability level of each of these components.

This will help you deal with the specific security issues anticipated in each one of the above components and put in place the right types of counter measures. This is necessary to ensure that the individual component you are dealing with operates with optimum efficiency and does not give rise to any security issues in such a way that the overall security of the network is compromised.

Some of the security issues connected with some of the above components includes:

- **Bridges:** In case of using a bridge you have to take specific counter measures to prevent a broadcast storm, in which all the broadcast traffic is automatically transmitted to all the connected networks in the bridge set up without verification of their MAC addresses. This effectively floods the entire network thus bringing a serious bottleneck in the smooth functioning of the data network. When an attacker creates a broadcast storm in a deliberate attack the security of the entire network is under threat and you must have good counter measure to deal with this situation so that you are able to prevent any data security breaches and the network is able to function at normal levels by automatically isolating the bridge under attack.

Switches: When using a switch as an intelligent Hub in a network, it uses MAC addresses to route traffic and is configured to transmit the data in a network only to the port that is connected to the destination MAC address. This creates network segments and helps in increasing data transmission rates to the level that matches with the individual network segments. Most of the times a switch are mainly used to create Virtual LANs or VLAN to logically segregate a network and limit the broadcast domains. Now switches are used in both network layer as well as in Application layer in a Data Network and you have to create the right routines to find out all the vulnerabilities of the switching technologies and their overall impact on the security of the network. This will help you build a good security protocol while using switches as basic component in your network.

There are many types of transmission of data as they happen as an analog transmission or a digital one. They use different types of transmission schemes like synchronous or asynchronous transmissions. They may be transmitted through a single channel making it a baseband transmission or through a multiple channels making it a broadband transmission.

What is sent through a data transmission medium is one of the following namely:

- An electrical voltage
- A pulse of radio wave
- An energized microwave or
- A bunch of infrared signals

All these basic characteristics determine the type of transmission and this takes information and data with it to the designated place through a combination of network components. This process is prone with so many vulnerabilities and possible attacks and as a person responsible for the ultimate information security and network security you must be able to address all the anticipated vulnerabilities to make your data transfer safe, secure and accurate at all times.

The transmission of data takes place through wired connections, or through wireless networks or through a highly optimized fiber optic cable. These form the media for the transmission of information through the network. These follow a number of protocols, standards and have to comply with many of the procedures set up for the transmission to occur and may pose serious security issues if not anticipated and provided for prior to or during and after the transmission of data .

You will be studying in detail about all these including the following while preparing for your CISSP test.

- Operation of hardware (e.g., modems, switches, routers, wireless access
- points, mobile devices)
- Transmission media (e.g., wired, wireless, fiber)
- Network access control devices (e.g., firewalls, proxies)
- Endpoint security
- Content - distribution networks
- Physical devices

3. Design and establish secure communication channels

The prime function of a CISSP professional taking in charge of the information and network security is to create a good design for the communication channels. Communication is one of the most basic requirements for a successful business. Though there should be controls and restrictions for the use of communication channels and media for security reasons, these cannot be too tight or completely rigid during the use of communication channels.

But, still you must be able to find the right designs for your network security systems and communication must be allowed to happen with reasonable restrictions and greater control over the anticipated security vulnerabilities so that no part of the data network or the information sent through are compromised in any way.

For this you must have a sound knowledge and understanding of various factors that determine the design and operation of a secure and fool-proof communication network. The communication in the present days may take many forms like

- Voice communication
- Multimedia presentations and collaborations
- Remote access facilities
- Data transmissions
- Data and information sent through a Virtualized Private Networks

Each type of these communications has their own set of devices and equipments and follows a set of protocols to deal with communication of these data types. The responsibility of a net work administrator is many-fold since he has to protect the confidentiality, availability and integrity of the data and information he is transmitting through the network. Apart from this he has to protect the network itself against attacks and vulnerabilities.

In this circumstance, it becomes necessary for the right type of designing of the communication network as well as operates them as per the set security criteria so that no security issue arises. Even when a serious security issue crops up, if the design and operations of the communication network are done as per the latest concepts of network security it will be possible for them to be suitably answered and fix the security hole in no time avoiding costly damage to the information security of the business.

Towards this you must have sound knowledge in the following topics

- Voice communications
- Multimedia collaboration (e.g., remote meeting technology, instant messaging)
- Remote access (e.g., VPN, screen scraper, virtual application/desktop, telecommuting)
- Data communications (e.g., VLAN, TLS/SSL)
- Virtualized networks (e.g., SDN, virtual SAN, guest operating systems, port isolation) etc.

4. Prevent or mitigate network attacks

The main function of an information security specialist includes the prevention and mitigation of network attacks. This must be done in an effective and efficient manner as the entire information of the business especially the ones that are critically important to it may be at risk. Only by preventing the security breaches one can easily avoid the loss of critically important data or hacking into the security system of the business.

In the present day global business scenario your Organization has to deal with varius types of hazards to the information security and you have to be very careful in designing, implementing and monitoring a good and fool- proof information security system.

An attack to the information security may be with the intent of just sneaking in and looking at things and may be passive in nature, which is less dangerous than an active attack which is far more dangerous as it is done with the intent of causing damage to the information security. When this happens there is a serious breach of the security protocol and it leads to alteration and stealing of data, make the data systems go haywire and make the data unusable and corrupted.

Some of the widely used information security attack modes are as follows:

Sniffing or snooping: this occurs when an attacker gains entry into the data path and he just listens in and read the flowing data and does not actively interfere with the information security system. This type of eavesdropping is possible only when the data or information flow occurs in a clear text format and no encryption is in use. This type of attack happens all the time and the best way to avoid this is to protect your information network with the use of cryptography techniques.

Modification of data: is a form of communication network attack which happens after the attacker has gained entry into the network and is able to get hold of the information that is being sent or received. After this he modifies the data and resends it without the knowledge of the sender or receiver. This type of attack is very dangerous as the attacker can do any modifications to the data as he wants and send it as if it was sent by the original sender. Encryption is the key for preventing such types of attacks.

IP address spoofing: in this type of attack the attacker gains entry into your network through a spoofed up IP address concealing his real identity. Afterwards he modifies, reroutes or deletes your data severely affecting the confidentiality, integrity and availability of your precious data. To avoid such attacks your information security system must be robust enough to find out the spoofing and deny entry, through carefully built TCP/IP protocols.

Password based attacks: in this type of attack the attacker gets the access information like username and password and gets into the network as if he is a genuine user and is able to gain entry as per the privileges of the original account holder. If the attacker is able to gain control of an admin level account then he is free to do anything he wants on your network and he can receive, reroute, modify and delete data on the server or even change the server configurations and prevent the other genuine users from entering into the network. This type of attacks are very common and they can be prevented by stricter access control procedures and implementing a double access controls. Even in case of an unauthorized entry the system must be able to identify the compromised account and deny access immediately.

Denial of service attack: has a serious consequence on the network as the attacker after gaining entry into your network initiates routines that prevent other users from using the system or network, and divert so much of false traffic that the network has to be shut down. This can be prevented by stricter access controls and by bringing in many redundant systems that prevent further damage to the network.

Like this there are so many ways to attack an information security system or a network and you must have enough knowledge and resolve to neutralize all these and save the integrity of the network in an efficient manner. [9]

[9] Domain 4 Podcasts

Domain No. 5

Identity and Access Management[10]

(Controlling Access and Managing Identity)

Overview

Identity management and access control is the next important aspect of the CISSP syllabi and it occupies a very significant place in the overall information security management. As the users of the system are the dominating factor having very deep impact on the design and management of information security systems, you have to pay very close attention to this core area in the overall security system of the organization.

The users and their ability to create, store, manage and handle vital data and information in a safe and secure manner forms the crux of the information security system. This domain of the CISSP certification material deals with the human element in the information security and the process of managing them for successful implementation of an effective information security system for your organization.

This domain lets you know how to provision the resources of information security among the users of the system and managing their identities, and giving them the right types of access control depending on their position in the organization to access and use the information in a secured manner. As such this domain is concerned with the human element of the information security system and how they are allowed to interact and function with the information security system you have created for the organization.

This domain explains how you have to design individual components that make up the total information security system with the right types of access privileges and maintaining the right identity management for easy and effective access to the information and data of the organization.

[10] Watch these videos on Identity and Access Management

Most of the attacks happen due to vulnerabilities and mismanagement of the identity management part of your information security system and hence you have to get very good knowledge in the modern concepts of identity management and access control. The main aim of this domain is to prevent the unauthorized access to the system and access the information by the unauthorized persons causing severe damage to the organization.

The CISSP professional is expected to have a very sound knowledge in the concepts of identity management and access control as it goes to the root of the information security system, for preventing the attacks and gaining unauthorized entry into the information handling system of the organization with malicious intent.

This identity management part of the CISSP curriculum aims to help you gain knowledge in and test your prowess in the following topics of

- Access management
- Identification authorization
- Identity management
- Authorization of users
- Authorization of systems and services for secured running of the information security system
- Different types of Authentication
- Accountability of users
- Managing Sessions while using the information security system
- Registration and proofing
- Federated Identity Management
- Managing of credential management systems

.

In addition to this you will be also tested on how to integrate third party cloud based identity management services as an integral part of ensuring the right types of identity control and access management. You will also have to be well versed in the concepts of on- premise identity services and how it helps in the maintenance of confidentiality, Availability and integrity of the information.

You will be tested for your knowledge and capability in implementing and managing authorization and access control mechanisms as a part of your overall information security system based on rule based mandatory access as well as discretionary control of access to the information security system. You are expected to have very good knowledge in the prevention and mitigation of attacks on the access control mechanisms you have created as a way of protecting the information security system, and prescribe the right types of routines for successful running of the identity management lifecycle.

Key Areas of Knowledge

1. Control Physical and Logical Access to Assets

Controlling access to the security assets is the core function of the information security and this is achieved through implementing the right types of physical and logical access. Threats to the information security in this modern computer and internet era needs to be highly sophisticated
and must be able to provide the right type of controls to safeguard the system from various types of attacks like

- Internet based attacks
- Computer viruses
- Trojan horses
- Insider attacks
- Covert channels
- Software bugs
- Honest and bona fide mistakes

To prevent these from compromising your information security system you must implement a comprehensive physical and logical control in respect of all the laptops, tablets, mobile devices and other types of end point devices the users of the system integrate with it.

Access control helps the Security system defined and controls the systems and resources a user can access and what he can do and what he cannot do on that permitted system or resource. This is implemented by the formulation of a set of rules or permissions and a combination of administrative, technical and physical controls. As the person in charge of information security you have to design, create and implement the following types of controls for better security environment like:

- Preventive controls to reduce the risk of data and information security lapses
- Detective controls for finding out the vulnerabilities, violations and incidents in the system
- Corrective controls for remedying the violations and incidents and providing suitable counter measures to prevent their recurrence
- Deterrent controls for discouraging the occurrence of violations and harmful incidents
- Recovery controls for resetting the system after an attack and restoring its normal functions without loss of time or integrity of the overall information security system
- Compensating controls to provide alternative and substitutive ways of bringing back normalcy into the system even after a serious attack

These types of controls complement each other in their functions and are geared towards better management of security issues and keep the level of information security in the organization at a higher level.

For ensuring better physical and logical access control you have to focus more on the following to gain enough knowledge about access management of

- Information
- Systems
- Devices
- Facilities

2. Manage Identification and Authentication of People And Devices

Any system put in place for assuring good Access control involve in providing right types of

- Authentication
- Authorization and

- Accountability

- Authentication is the process of allowing the access into the system after due verification of the identity of the user. As such this is essentially two step process of identification of the user and authentication of their identity by presenting a pre- allotted specific identity criterion to the system. Authentication is the process of accepting one's identity and allowing him to enter the system in a legal and permitted way.

- Authorization is the process that defines the extent and nature of rights an authenticated user can enjoy inside the system.

- Accountability is the process that creates the necessary capabilities in the system that is able to associate the users with their actions and their impact on the overall security of the system.

These are designed and implemented as system based access controls that provide first line of defense against attacks and are put in place to protect the entire information security system.
The next type of access control is the data access controls and are created and implemented to protect the data in system.

The authentication of users in the system can be done through asking for

- Something you know like a pass word or an personal identification number
- Something you have like a token or a smart card
- Something you are like the use of voice recognition, retina scan, or scanning your biometric data including iris characteristics

The process of personal authentication using these may be either two factor authentication requiring two of the above three factors or a three- factor authentication for all three factors for authentication. The authentication system you build for your system must be a strong one with at least a two factor authentication requiring at least two of the three factors and this provides a fairly good authentication for those who want to use your information security system.

The identification and authentication is of paramount importance for maintaining the required level of security of the overall information security system and hence as a CISSP certified professional you must be able to create the right types of identification and authentication routines to ensure the confidentiality, integrity and availability of the data. For this you have to gain more knowledge in these topics:

- Identity management implementation (e.g., SSO, LDAP)
- Single/multi-factor authentication (e.g., factors, strength, errors, biometrics)
- Accountability
- Session management (e.g., timeouts, screensavers)

- Integrate Identity As A Service (e.g., Cloud Identity)

Ensuring proper identity of a user to get access into your information security system is very important especially if you are using cloud based data storage and computing system. You have to put the right types of services to do this and fortunately there are many identity–as- a-service offerings that will help you have a fool-proof identity authentication system in place with little effort.

You have to find the right type of cloud- based identity and access management solution, or use a Identity as a Service (IDaaS). This must be able to deliver the following features like

- Single sign-on
- Password management
- Provisioning
- Access certification services for your Cloud environment
- Access certification for your mobile devices
- Access certification for on- premises Applications

This System must be able to offer the required level of security, scalability, availability and performance to match the needs of your information security system. The IDaaS solution you are creating for your system must be able to provide a cost- effective, fast and easy to use solution with good usability through a simple, and intitutive user interface. This must be able to connect well with other cloud based and internal on- site as well as Web based Applications.

Some of the requirements for a good IDaaS serviced are

- Ability to provide single- sign- on for seamless sign- on experience through any device
- Easy and effective pass word management
- Excellent user provisioning for streamlines process of creating, revoking and changing user access based on various factors
- Easy and automated access certification
- Easy to use with very narrow learning curve
- Comprehensive reporting and Audit functionality
- Ability to connect to and manage all the resources in your information security system
- Scalable in nature to accommodate your growing needs

> “CANDIDATES ARE EXPECTED TO BE CAPABLE OF IMPLEMENTING AND MANAGING AUTHORIZATION MECHANISMS INCLUDING THOSE BASED ON ROLE-BASED, RULE-BASED, MANDATORY AND DISCRETIONARY ACCESS CONTROL.” *~CISSP HANDBOOK*

So, focus on these vital points to make your identity authentication process as secure as possible without putting the genuine users to face problems during their day to day use of the same. As a CISSP certified Information security professional you must gain necessary knowledge in this regard to tackle all security issues that may arise during the user identification and authentication system.

- ❖ Integrate Third-Party Identity Services (E.G., On Premise)

If you are not able to develop an identity and authentication application by yourself the next best option is to use a third party identity services available now. This will simplify the identity authentication process. However, you have to make sure that the third- party identity services you are getting for your organization satisfy the following namely:

- **Availability:** the service must be available all the 24 X 7 and the genuine users of your system must be able to use it at any time as it is the primary point of contact for them to get into the system. If it is not available they will not be able to get into the system at all.

- **Must be able to work with all the required resources:** the identification service you are using must be able to work efficiently on the basis of all the requirements available as per the industry standards

- **Compatibility:** the primary aim of using a third party identity service is to simplify the sign- in process for your users over the cloud environment and the service you have chosen must be able to work with all other similar services for added compatibly and simplicity of signing in service.

As these third- party identity providers have very high level of security built into their products you can get a good headway for providing a secure sign- in process for your system users. Know more about these and try to select the one that is best for your system.

The access control and identity authentication in an organizational information security system may be either role based (RBAC) or Rule based one. In a role based access control the access to the computer or network is regulated based on the roles of the individual users and they will be allowed to perform specific tasks on the system based on their job competency, authority and responsibility. In the Rule based access the access into the system is controlled by the pre-determined rules of the organization and help the information security system to enforce its access control through well defined rules.

To ensure the security of the system you can implement a good discretionary access control (DAC) with clear specification of who can access what in the system based on the discretion of the system admin. Yet another mode of access control is the mandatory access control (MAC) and this has well defined specifications allowing which user can access which sets of data ensuring that not all of the users have access to all the data in the system.

So, you must have a good knowledge of various types of access controls that enhances the security of your overall system.

- Implement and manage authorization mechanisms
- Role Based Access Control (RBAC) methods
- Rule -based access control methods
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)

❖ Prevent Or Mitigate Access Control Attacks

The main objective of an attacker is to attack your access controls and gain unauthorized entry into your system. There are many types of attacks and some of the most common are:

- **Brute force attack:** in which the attacker tries all combinations of letters, characters and numbers to find the password or passphrase or PIN to log into the system. Here he can use many hacking tools available now and given sufficient time he can achieve his objective. The right way to protect this type of attacks is to deny the availability of the password file or database.

- Dictionary Attack: this is a type of brute force attack in which the attacker is more focused in cracking the password with a pre-defined word list. Here he uses word lists or dictionaries available on the Web and tries to gain entry into the system by using password cracking utilities like L0phtcrack or John the Ripper, which are fast in their action. This helps them crack the password database within a short time and gain entry into the information security system, to fulfill their bad objectives. This type of attack can be prevented by protecting the database of passwords or files in a secure manner.

- Rainbow table attack: here also it is a form of brute attack, and the attacker takes the password file or database and compares the hash of the passwords with a universally available hashes table which converts the hashes into their corresponding plain text equivalents. To prevent this type of attack “salt” your hashes and store them at a very secure place.

- Stack- overflow or Buffer overflow attack: this is like a denial of service attack and here the attacker enters the system in an unauthorized manner when he makes an application or a protocol in the system to cause overflow of data by making it to store more information than it is allowed to do. This makes the data already stored in the location get corrupted, and crash the application leading to unexpected or unpredictable behavior of the information security system. This type of attack is very common and is capable of causing more damage to the entire IT infrastructure of the organization. To mitigate this type of attack identify the vulnerabilities as early possible and take decisive steps and counter measures to prevent such attacks.

Apart from this there are many other types of attack like Man- in-the-Middle attack, Password sniffing, session hijacking, social engineering, etc.

To prevent such attacks you have to follow systematic approach by doing the following:

- Simulate the attacks to identify the vulnerabilities and weak spots in your network by threat modeling
- Carry out honest asset evaluation to determine the level of overall security
- Do a thorough vulnerability analysis
- Conduct a source code review to find out the state of health of various applications and protocols
- Create an access aggregations simplifying the access controls

A CISSP professional must know how to prevent such attacks on the network and must be prepared to prevent the damages in case an attack occurs and help to recover as early as possible. Towards this you are expected to have a good knowledge about how to Prevent or mitigate access control attacks.

4. Manage the identity and access provisioning lifecycle (e.g., provisioning,

Review)

For protecting the security of the network it is necessary to put in place the right types of account provisioning, review and revocation. This involves in the following phases of IAM provisioning lifecycle:

Role design, creation and review: in this phase of early stages of development, configuration or customization of the security system each role of the users are defined. This is reviewed periodically to ensure that they are appropriate and safe for the overall security system

Access provisioning: there should be good and formal ways of requesting access to the new users who want to have access to the network resources. This methodology must be secure and be able to maintain the overall security protocols set for the system or network.

You need to have good knowledge of these to assure safe and secure operation of your network and information security system with a higher degree of security.[11]

[11] Listen to these Domain 5 Podcasts (Streaming)

Domain No. 6

Security Assessment and Testing[12]

(Designing, Performing, and Analyzing Security Testing)

Overview

An information security system has to face many types of risks and may have adverse impact on the overall security of the information due to various factors. These risks to the system leads to vulnerabilities and these in turn lead to breach of security. As a CISSP certified person you must know where and how to look for and identify these risks inherent in the system and analyze them in detail to find suitable solution to each one of them before they lead to security issues.

Security assessment and testing are very vital to the success of information security in any system and hence these two concepts occupy an important place in the CISSP curriculum and are added as a separate knowledge domain. The deep study of these topics is necessary as they form an integral part of the certificate exam. You also need to gain knowledge when entering into the information security system creation and management when you begin working as a CISSP certified professional later.

In an information security system, you will find that there are many assets and these are the basic components that make up your overall security system. Each one of them is prone to risk factors and evaluation of their nature, extent, and type of risk associated with each of them becomes a necessary task for taking the required action. For this you have to use some of the tools and techniques to counter the actions that may jeopardize the information security in the organization.

Some of the types of anticipated risk factors include:

- Architectural issues that arise due to incompatible system components or those that arise due to weakness in their construction or functioning

[12] Domain 6 Videos

- Design flaws that come into play due to poor or bad design of the information security system
- Configuration errors due to improper setting up or inability to operate the assets as per the set security criteria
- Hardware vulnerabilities due to poorly designed components and subsystems or those cannot function at the level anticipated
- Software issues due to poorly designed software applications, or those that are infected, or affected by malicious programs and include bad patches in the coding

Apart from this the action of the organization itself in formulating its

- Security policy plan for effecting fool- proof security
- Defining of various security processes
- Procedures for affecting the security processes etc

and other weaknesses arising from known or unknown sources may affect the security of the information system, and this makes the system unable to deliver its intended functionality in a safe and secure manner.

While preparing for the CISSP certification you must know how to conduct the continuous evaluation of the risk factors and must be capable of validating the assessment and test the strategies that are necessary to maintain the required level of security of information system to provide for the tirade of confidentiality, availability and integrity of the information.

To be a successful information security professional you are expected to have sound knowledge on the concepts of

- Conducting vulnerability assessments
- Know how to conduct penetration testing
- How to run synthetic transactions
- Go for code review and testing
- Deal with misuse cases
- Run interface testing

You must know how to ensure that security policies and procedures put in place for safeguarding the information security are applied in a uniform and consistent manner to ensure the high level of security of the information system. You will be also responsible for ensuring the plan for business continuity and disaster recovery are created, maintained, updated and will be kept ready for immediate implementation in case of a disaster. For this you will be held responsible for the collection, analysis and formation suitable processes and plans based on the security process data.

You must be prepared to be tested for your knowledge and skill in the following areas including:

- Account management
- Management review
- Evaluation of key performance
- Study of risk indicators
- Verification of data and information backups
- Training of staff and creating awareness among users about the risk factors and the security process that are running
- Plan for and implement the disaster recovery
- Plan and implement processes for business continuity

You must know how to respond to the security evaluation and assessment and must be able to conduct honest, to the point and focused analysis and prepare concise reports on the same. This is necessary for creating the right types of mitigation strategies for implement them for prompt action towards maintaining the information security.

A key capability that is expected from the CISSP certified person will be the ability to analyze the risk factors and prepare the report based on the test outputs. You must also ensure the conducting of and facilitating internal security audits as well those conducted by third parties.

Key Areas of Knowledge

1. Design and Validate Assessment and Test Strategies

It is necessary for any organization to get the right type of security for its vital information and data. For this they need to follow and implement sound information security systems. A CISSP certified professional is fully trained to do this in a better way and for this they are taught how to design secure information handling systems and manage them without any security issues.

In the present days of information explosion era, the security threats are everywhere and are constantly evolving in nature, potential and extent. For this you must be well versed in the ways of detecting the vulnerabilities in your information security system and provide for the right ways of countering them so that the security of the information is ensured. You have to have a thorough understanding of the various components and elements that were assembled to make up your system and their weaknesses.

As the strength of a chain depends on the strength of its weakest link, so does your information security system and it is as secure as the security of your weakest component in your security system. To know how to make your system more secure and safe for the organization you must know how to

- Develop working assessment of the information system and do the assessment in a consistent manner
- You must have the ability to evolve suitable strategies based on the results of the assessment to counteract any vulnerability in the system
- Do the testing of your strategies and apply them to real life situations and find out the shortcomings in your overall strategies
- Conduct the assessments as per the changed strategies and find out results of the changes you have made
- Do various types of tests like penetration testing on a continuous basis to see the strength of your security system
- Create the right type of management controls, operational controls and implement them at the right time and constantly monitor their effect on the overall security system
- Conduct the tests at regular intervals and take the outputs, study them and come out with security updates in an comprehensive way
- Collaborate and work with security Auditors both internal as well as third party Auditors and come out with the right security criteria as per the perceived threats to the information system

These form some of the basic functions of a CISSP certified Information security professional and for this you are expected to have sufficient knowledge in the following concepts of how to Design security system tests and conduct and validate assessments. Create right strategies to tackle any security issues and test strategies for counter acting any security issues.

2. Conduct Security Control Testing

Conducting security control testing is one of the primary functions of a CISSP Certificate holder who is responsible for the security of the information system. The process of control testing involves in taking into account various elements and individual components that have been assembled to work as a single security system. As each of the components has their own level of security issues a thorough vulnerability study on each of them is a must before you can arrive at a comprehensive vulnerability and the anticipated threat perception for the whole information security system.

> "CANDIDATES WILL BE TESTED ON VULNERABILITY ASSESSMENTS, PENETRATION TESTING, SYNTHETIC TRANSACTIONS, CODE REVIEW AND TESTING, MISUSE CASE, AND INTERFACE TESTING."
>
> *~CISSP HANDBOOK*

To do the vulnerability assessment you must be well aware of the security problems that may crop up from each one of the components and factors of the system and these have to be added together to arrive at the overall vulnerability assessment. Once this is done, you can be confident of facing the threats with the right types of counter measures to deal with each one of them in a fitting manner so that you are able to maintain the required level of confidentiality, integrity and availability of the information that is being dealt with by your security system.

There are many ways to do this and you have to be well aware of penetration testing and the routines you have to follow to complete this effective way of vulnerability assessment to identify precise levels threat possibilities, and take right steps at the right time to counter the vulnerabilities found in the system. Yet another way of finding possible failures of the information system components is by conducting log reviews for finding out the health of each of the hardware components that are working in your system. You have to conduct the log reviews of various security procedures you have put in place to make sure that they are working in the way you wanted.

Another way of conducting security control testing is by running synthetic transactions on the system elements and find how they react in case of an attack and implement necessary corrective steps in case of a possible security issue. You should also concentrate more on code review and testing as most of the modern security systems run through software applications. When there is an issue with the coding of the software application it can lead to serious security issues later. So you must know how to conduct the code reviews and testing to ensure security of your information system.

Misuse case testing is also done on the parts and users of the security system to know their preparedness for facing security threats and this will show how the system will react and act to prevent misuse of the security routines. This is necessary to prevent malicious attacks on the system and you have to be well versed with the ways of testing on this important aspect and are able to put in the right types of security controls for adding strength to your security actions.

A Test coverage analysis helps in finding the extent of testing that is carried out to ensure the implementation and operation of the right type of security controls. This will determine whether the testing you are conducting on the system is able to give the necessary inputs for the vulnerability assessment of the system. Based on this assessment you will have to take the vital decision of going for extended testing routines and put in more security controls to make sure that all your security protocols are running perfectly to protect the information security system from all possible threats, attacks and vulnerabilities.

An interface testing is also necessary to find out the vulnerabilities that may arise during the use of interaction with the system through the API, User Interface and physical contacts with the components of the security system. This will make sure that the interfaces through which we are operating the security system are running as per the security guidelines you have implemented.

Thus a detailed study of the following topics forms an integral part of your preparation for CISSP certification:

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing (e.g., manual, dynamic, static, fuzz)
- Misuse case testing
- Test coverage analysis
- Interface testing (e.g., API, UI, physical)

3. Collect Security Process Data (e.g. Management and Operational Controls)

Collecting security process data is the backbone of any security system and it is vital for assessing the health of your information security system. The collection of the data must be done as per strict rules as it is one of the vital aspects of the security system. This is the earliest indicator of possible vulnerabilities and will be able to give opportunities for a CISSP certified information security specialist to find the possible security issues and decide what type of corrective actions must be taken to protect the overall security of the system.

The process of collecting data from your security system may be done in many ways and these must be well documented and be able to give you all sets of data for conducting a comprehensive security data analysis. You must also conduct complete management review to know the readiness of various aspects of security management systems you have implemented to protect the health and security of your information system. This is necessary to know how the factors that are added to the system to manage the security functions are effective to prevent the threats and attacks on it.

Yet another important function expected from the CISSP certificate holder is the performance analysis of the system. As the health and security of your information security system depends on the performance levels of each of the individual elements you have put together to make up the security of the whole system, you must monitor the performance each of these items and compare them with the standard benchmarks you must know how to take immediate corrective actions when you find shortcomings. To do this you must be aware of the risk indicators and take their values to find out the performance anomalies of the elements and replace them in case they fail to meet the standards.

Back up of critical data must be done on a regular basis and it must be made a continuous process as an important part of the overall security set up. As anything may happen to the system at any time you have to plan for verifying the backup data on a regular basis so that no loss of data occurs in case of a security attack.

Training and creating awareness among various classes of users must be undertaken as a part of the security operation. This is necessary for making every user of the system aware of the risks involved and the vulnerabilities anticipated in the information security system. Once this is done the users can be easily educated to run the security operations and take preventive actions to avoid data loss or security breaches automatically without waiting for the interference of others. This also enables the users to operate the system as per the set security protocols for safety and security of the information security system.

Disasters may happen at any time and most of them happen when you are not expecting them to happen. Disasters with respect to the organization may be both natural as well as man- made and some of them may be so serious as to affect the very existence of the organization. Such things must be anticipated at all times and you have to run your information security and physical security of the organization in a state of readiness to meet any type of disaster and come out of its bad effects within minimum time and with minimum damage.

This calls for extensive knowledge in disaster management and recovery and the creating a set of fool- proof strategies for business continuity. As this matter goes to the very existence of the organization you are expected to have very good knowledge in the concepts that relate to the business continuity and disaster management during your study for CISSP certification.

- Account management (e.g., escalation, revocation)
- Management review
- Key performance and risk indicators

- Backup verification data
- Training and awareness
- Disaster recovery and business continuity

4. Analyze and Report Test Outputs (e.g., Automated, Manual)

Risk analysis and report preparation are some of the important functions of an information security professional. You have to conduct various types of analysis to take stock of the overall security situation in your organization and based on the reports you prepare, you will come to know the types of anticipated threats and the impending vulnerabilities that have to be adequately taken care of. Thus, the report preparation is an essential skill and during your study for the CISSP certification you will be able to get the necessary exposure in the ways of analyzing various factors that are likely to have a bearing on the overall security position and how to tackle them in an effective manner.

5. Conduct or facilitate internal and third party audits:

Audits are a part of day to day routine of an organization and they are the indicators of how your information security operations are functioning. There are various types of audits that are conducted both by internal auditors as well as by external third party auditors. As the man responsible for the smooth and effective functioning of the security system you are expected to take an active role in these audits. You have to prescribe the nature, type and criteria for security audits and you have to provide all the relevant data and information to facilitate the due conduct of audits.

As a part of the internal training and awareness programs you have to conduct internal audits to know the level of knowledge you have imparted to the different levels of users about the type and extent of security operations you are carrying on in your organization. Based on these audit reports you will be able to determine the effectiveness of the training and take remedial actions.

There are periodical security and other types of audits conducted by various agencies partly as a way of routine procedures of the organization and partly as compliance to legal regulations. These audits are to be conducted as per legal procedures and the reports are to be filed with governmental and other authorities.

Here also you will be helping the external auditors to have a thorough audit of the security aspects of the organization and based on their report you have to take corrective actions to make your security system function with utmost confidentiality, integrity and availability at all times.[13]

[13] Podcasts on Security Assessment and Testing

Domain No. 7

Security Operations[14]

(Foundational Concepts, investigations, Incident Management, Disaster Recovery)

Overview

In the present day competitive business scenario security of information is paramount to a business. Due to this, information security has evolved into a separate branch of study. The CISSP certification lets the world know that you have sufficient knowledge and skills to protect the information and the information handling systems from being attacked by various factors. The security operations forms part of the CISSP curriculum as one of the domains and it has many topics that are necessary for the information security specialist to have good grasp of.

This domain lets you study in detail the topics that correspond to the operation of security systems that are geared towards maintaining the confidentiality, integrity and availability of the information which forms the tirade of the information security. Here, you have to study in detail the various security concepts that must be applied for maintaining the information safety. You will be also studying about various operations that must be successfully and consistently undertaken to run the enterprise computing systems with information security as their main goal.

The study of topics covered under this domain mainly relate to the practicalities connected with the tasks and situations that may arise during the operation of information security systems. These topics will make you aware how an information security professional has to tackle these situations and successfully safeguard the information security systems of the business. These are the concepts that you will be using on a daily basis during your work day and will be focused on how to anticipate a vulnerable situation and how to deal with them

[14] Video Playlist on Domain 7: Security Operations

and place the right types of counter measures to save the information from external malicious attacks as well as natural and man made disasters.

It is practical in nature and intended to cover the tasks and situations that information security professionals are expected to perform or are presented with on a daily basis. It is also representative of the areas where security professionals spend most of their time so it is no surprise that the security operations domain is the largest in terms of individual topics on the CISSP examination.

Forensic investigations are a part of the information security domain and you as a certified professional must have sufficient knowledge in all the concepts that will aid in conducting such investigations.

You must also have good knowledge on the latest investigative concepts like

- Evidence collection
- Evidence handling
- Documentation of investigation processes
- Reporting for investigation operations
- Techniques of investigations
- Digital forensics

It is also necessary to understand and be well aware of various requirements for investigations of the following nature like

- Investigation on civil matters
- Criminal investigations
- Operational investigations
- Investigations relating to regulatory matters

There are various security functions that form part of the duties of a certified CISPP professional for the proper upkeep of the information security and among them efficient logging and close monitoring of

“IN ADDITION TO SUPPORTING FORENSIC INVESTIGATIONS, LOGGING AND MONITORING PROVIDE VISIBILITY INTO THE DAY TO DAY OPERATION OF THE INFORMATION TECHNOLOGY INFRASTRUCTURE.” *~CISSP HANDBOOK* the security systems are the most basic and vital among them. The basic functions of logging and monitoring play a multiple role in the overall information security administration and management.

These functions are necessary for knowing the state of and following the real condition of the security elements during their day to day operations. They are also needed for supporting the ongoing investigations. They help you to know the real health and effectiveness of the systems that make up your information technology infrastructure.

The logging and monitoring cover a wider range of concepts like

- Intrusion detection for preventing attacks on the information security system
- Prevention of intrusions to safeguard the safety and integrity of the information
- Collection and processing of security information
- Handling of event monitoring and reporting systems
- Protecting against the data leakage etc

The security operations you have set up and running for the upkeep of the information security systems need resources to perform efficiently. It is the duty of the CISSP professional to know in detail various aspects of resource provisioning for the security systems. You must also know how to efficiently manage, handle and operate these resources in such a way they are able to give the required power and energy to run the security systems in a flaw less manner. It is to be noted that these resources must be made available to the security system during their entire life cycle, as the entire information security system is based on these resources for their running efficiency.

A CISSP certified professional is also expected to have the necessary exposure and knowledge about the creation, setting up of, managing and maintaining various types of protective controls that have been integrated into the information security system. The preventive controls about which you are expected to have deep knowledge include

- Firewalls
- Intrusion prevention systems

- White listing of Applications
- Installation and setting up of anti- malware and anti- virus applications
- Using of honey pots and honey nets
- Sandboxing etc

You must also know how to enter into and managing of third party security contracts and related services for maintaining the information security systems and applications. Apart from this some of the additional requirements of knowing about patches, vulnerability inherent in the system itself and those that have to be anticipated from external sources must also be thoroughly studied for your certification exam.

There are many additional topics that must be studied in detail under the security operations domain like:

- How to respond to incidents in the information security system
- Taking steps for early recovery of the system from the incidents
- Recovery from disasters both natural as well as from man- made ones
- Ensuring business continuity by ensuring early recovery and rapid disaster recovery
- Conducting of processes that are necessary for the incident management
- Create the right types of disaster recovery processes
- Testing and assuring the adequacy of the recovery processes
- Participating in business continuity planning

This domain also deals with the topics on ways of ensuring physical security and ways of protecting the personal security of the users of the information system in the organization.

Key Areas of Knowledge

1. Understand and Support Investigations

Investigations are a part of the information security management and you have to conduct or support the conducting of investigations by other agencies within or outside of the organization. Whenever there is an attack leading to a breach of security, you have to find out how this attack was possible and who did it and for what they have done it. You have to find out the damages caused to the information systems and find ways to tighten the loop holes if any found in the system.

When the attacks are criminal in nature the law enforcing agencies conduct investigations to find out the culprit or if a civil action has taken place then investigations are done to find out who was at fault and how much is the loss caused and who has to compensate whom etc.
All these investigations are based on the information security systems you are operating and the actions or omissions that have been conducted on them. So, you must take an active role in conducting the investigations or support the investigations conducted by others.

As this is an important function with respect to the management of information security systems you must have good knowledge about various aspects of investigations and the things you have to do and those that you should not do.

All investigations have the common purpose of evidence collection and it is your duty to help others in the process of evidence collection. So you should have sound knowledge on

- Types of evidence like direct evidence, physical evidence, documentary evidence or demonstrative evidence
- Rules of evidence like best evidence and hearsay evidence rules
- Admissibility of evidence by business records exception principle
- Chain of custody
- Evidence life cycle that involves in the collection and identification, analysis of evidence, Storage preservation and transportation, presentation in court, return to victim or owner

Report preparation and documenting the outcomes of the investigations is also an important function of a CISSP certificate holder and for this complete and accurate record keeping is must and it must be done for each of investigations held in the organization. The report of an investigator is the final record of the investigation and hence must be properly documented for future use as well as for compliance of various legal and procedural compliances.

Hence it becomes important for you to understand the necessity for acquiring the required knowledge about the ways of preparing the accurate reports of investigations and the information it must contain.

There are many techniques to conduct investigations and it must be started as soon as the incident or information related crime has come to light. It is a convention to treat all the incidents as an information security crime unleass otherwise proved. Various investigation techniques are used dpending on the goals to be achevied through the investigatin, or the demands of the relevant rules, regulations and legal requirements in a particular situation. You should be well aware of the investigaion techniques like root- cause analysis, incident handling etc.

Knowledge about all the investigation techniques is necessary so that you can slect the one that is needed to contain the damage caused by the incident without delay. As the investigation is going to be the first step in securing the information system from the adverse effects of the attack or crime, you have to select the right investigation technique that yields quick and effective ways of both stopping the attack and preventing its effects affecting the whole system.

In the present days of computer era, we are living in a digital information explosion and we are flooded with digital data of every kind. As an information security person you must have sound knowledge in the Digital forensics. You will be dealing with digital data and information in a digitized format throughout your work time. The information system you are building for your organization must be geared towards maintaining the confidentiality, availability and integrity of digital information.

A major part of your endeavor will be spent towards integrating various devices, and information handling processes to create, manipulate, store and handle digital information. Whenever there is an incident on your information security system you should be well equipped to launch the right type of digital forensics to get to the root of the crime or incident and take prompt steps to stop it immediately as well as arrest its effects causing damage to the overall information security system.

For this you must acquire good amount of working knowledge about various types of devices and modes of handling the digital data like digital media, data networks, and software applications that run these devices as well as embedded devices that form part of the information security system.

- Evidence collection and handling (e.g., chain of custody, interviewing)
- Reporting and documenting
- Investigative techniques (e.g., root-cause analysis, incident handling)
- Digital forensics (e.g., media, network, software, and embedded devices)

2. **Understand Requirements for Investigation Types**

A CISSP candidate must be well versed in the investigation requirements to handle any type of situation. This depends on his ability to look for the right set of protocols and put them in motion as soon as an incident takes place on the information security system. The types and techniques employed for investigation may change depending on the type of attack and goals of the investigation. You must be able to clearly identify the requirements for each of the investigation types and provide the right type of support to carry on the investigation and come out with its desired outcomes in an effective and prompt manner.

You must be in total control of the operational requirements of investigations and have them built in the system. They must be able to be launched in a swift manner in case of their necessity. The system must have been built on the principle of swift response in case you need it to respond to an investigation request or you need to launch an investigation to deal with an attack or commission of a crime on the system.

The operational requirements of investigation must be well defined and standardized to provide for the desired outcomes to the investigation whenever they are launched. For an investigation to proceed as planned it must be based on some sound protocols. These in turn are based on the set of requirements and the design of the investigation
Techniques that work on the strength of the operational requirements you have set for the investigators to work and reach their goals with meaningful and efficient outcomes leading to concrete results.

In case there is a criminal incident that is to be taken to the law enforcement authorities then the investigation will be conducted by external governmental agencies in a formal manner. You will be expected to co- operate with them and submit all the required documents and information for the investigation to be completed as per law. This calls for deciding on the requirements for the criminal investigation and comply with all the demands of the law enforcement agencies.

This calls for sound working knowledge in the functioning of the cyber crime cell and the latest developments in this field so that you will be able to meet the requirements that are necessary for a criminal investigation.

Loss or breach of information security may lead to civil liabilities for or against the organization you are working for. Most of the times this will be based on contractual liabilities and hence you must have a good knowledge of the law relating to contracts in your place and you are expected to gather all the requirements to meet this type of investigations usually conducted in a court of law or an agency appointed under their authority or an arbitrator empowered under the contract between the parties.

Every organization conducting a business must have to comply with various legal provisions, rules and regulations of the government or by the departments working under the same. There are many submissions and information submitted to these on a periodical basis. Apart from this, there are many special directions from these agencies for additional or special information. As a way of compliance of these you will have to be aware of the requirements for preparing the reports and datasheets to be submitted for legal compliance.

In the present days of electronic data in a digitized format making discoveries for the purpose of conducting investigations differ much from the conventional ways of making discoveries during the course of an inquiry. As a CISSP professional you have to be well versed in the ways of assisting eDiscoveries and help the investigating agencies get the full set of information they require for completing the investigation.

Hence you must concentrate more on the following topics and understand and create the requirements for investigation types

- Operational
- Criminal
- Civil
- Regulatory
- Electronic discovery (eDiscovery)

3. Conduct Logging and Monitoring Activities

As a part of maintaining the information security system integrity there are many types of access controls. These help in maintaining the right type of security of the system and help the users access and manage data in a safe and secure environment. To make sure that the access controls that are set up to achieve this are working in the way you have planned and to know the vulnerabilities residing in the system, you have to log each and every interaction that is taking place between the organization and the users of the information security system. This becomes the basic record based on which you are going to build your security system to make it fool proof and failsafe.

When you have initiated a proper logging system for ensuring the secure running of the information handling system, you can pin-point the problems that are occurring in the system and their source with reasonable certainty. Once you have a very efficient logging system in place you can be sure of finding the condition of the information security system and will be able to remove the security routines that are not functioning as expected or bring in new security protocols to fine tune the system for higher levels of security.

Monitoring of the information system is a vital role played by an information security specialist and this is a part of the logging activities that has been built into the system itself. Close and consistent monitoring is very essential for the proper functioning of the security system and by doing this you will able to easily anticipate the problems that are likely to arise through a particular element of the system.

By creating a super responsive and high efficiency logging and monitoring protocols in the system you will be able to provide more inputs into the business continuity plan and the disaster recovery plans. So, as a CISSP certified professional you are expected to have a deep knowledge in the methodologies and resources needed for good logging and monitoring activities.

As a way of closely monitoring the functioning of the security system there will be various types of intrusion detection and prevention systems integrated into the information security system. These systems are meant for real time monitoring and easy analysis of the network activity. This is useful in preventing potential vulnerabilities escalating into the full blown security issues. As they are able to provide a real –time monitoring and reporting you will be able to take immediate steps to address the happening of the attacks.

These intrusion detection and prevention systems play a very vital role in maintaining an enhanced level of security in the system and hence a study of these systems and their way of functioning and how they can be used to achieve the final goals form part of the CISSP knowledge area.

In this respect you need to study about various types of intrusion detection and prevention systems like

- active systems
- passive systems
- Net- work based systems
- Host based systems
- Knowledge based systems
- Behavior based systems

Getting the necessary security information on a consistent basis is necessary for the information security specialist to know the state of health and the condition of the overall system. This helps him find out the vulnerabilities and weakness of the components that are working together to ensure that there is required level of security in the system. The system must be so tuned as to get all the required security information so that suitable counter and preventive action can be taken to mitigate any adverse eventualities that may occur in the system.

When you have put in such measures and protocols that have automated security information delivery systems, the system can be saved from any possible attacks as the security information available will be able to give a clear understanding of what is happening and what to expect in the near future. With this vital knowledge, it is possible for proper and effective event management to save the system from total crash or be liable to be affected by man- made disasters.

Security information helps the organization in building a fool proof disaster recovery planning and business continuity planning. Armed with the latest security information you will be able to find suitable solutions for each of the anticipated vulnerabilities and disasters that have the capability to threaten the existence of the organization.

Getting the right security information at the right time is the crux of any information security system and it is vital for a CISSP candidate to study deeply the

- Types of security information that must be taken from the system
- Design suitable security routines to extract this security information
- How to analyze the data
- How to prepare concise and to the point security reports
- Find out the vulnerabilities and anticipated events
- Putting in place the right counter measures and preventive actions

Continuous monitoring is the process of monitoring the performance of the information security system whereby the functioning of the security controls are ensured to be running within the set parameters. This is set to run on an ongoing basis and feedback of the system helps the personnel running the system to know about the changes that occur in the system as and when they happen so that they can take note of the impact of these changes on the overall security of the system as soon as the changes take place. The continuous monitoring process goes on until there is a need for reaccreditation occurs due to changes that have modified the security controls already running or due to change in federal or agency policies that require reauthorization.

During this continuous monitoring process you need to take care of the following processes namely:

- Undertaking the configuration management and control of various security controls
- Continuous verification and authentication of ongoing security controls
- Creating status reports and writing the necessary documentation for the same

Apart from this the continuous monitoring also involves in the process of disposition of information, monitoring of the hardware elements and overseeing the functioning of the software applications. This also covers the other functions like moving of data, its archiving, discarding of information and destroying information in a safe and secure manner. This phase of information security also takes care of the sanitation of hardware and software systems for efficient risk management while disposing them. The residual data must be handled in a secure way so that the migration of system elements does not lead to any security issues.

It is necessary to extend the continuous monitoring process to configuration management and the related security control activity. When there is necessity to make changes to the information security system, then first the changes proposed are properly documented and then their impact on the security of the overall system is determined and proper actions and security routines are also changed in a comprehensive manner to maintain the same level of security before changes were made to the information security system.

Egress monitoring refers to the security controls that have been established to monitor and control outgoing traffic. The main aim of this type of security control is to prevent unauthorized data transfer, data exfiltration heavily compromising the security of information of the organization.

There are many ways to do this and some of the most common among them are the

- **Prevention of steganography attempts:** by this process an unauthorized transfer of data takes place by concealing the data to be transferred clandestinely inside or along with the authorized data. The concept of steganography is well developed and is widely used as a tool for unauthorized transfer of data creating a serious information security breach. So, this type of attempts must be carefully monitored and each transfer of data to outside of the organization must be carefully analyzed and the contents of the transfer closely monitored to make sure that the information authorized to transfer does not contain any other data.

- **Data Loss prevention systems:** these are well developed in the present days with capabilities to monitor, scan and detect particular data based on various criteria. When you have this type of system in your security set up, then you can configure them to detect, scan and prevent the transfer of data from your information storage and handling systems.

- **Watermarking:** is the process of adding id parameters to the data holders so that you can easily identify them and prevent their use outside the organization in an unauthorized manner.

Thus, this domain contains very critically important information and the concepts for effective security operation and hence the candidates opting for CISSP certifications must pay more attention towards this and acquire thorough knowledge about the various concepts that are in use to enhance the overall security of the information system.

- ❖ Intrusion detection and prevention
- ❖ Security information and event management
- ❖ Continuous monitoring
- ❖ Egress monitoring (e.g., data loss prevention, steganography, watermarking)

4. Secure the Provisioning of Resources

- ❖ Asset inventory (e.g., hardware, software)
- ❖ Configuration management
- ❖ Physical assets
- ❖ Virtual assets (e.g., software -defined network, virtual SAN, guest operating
- ❖ systems)
- ❖ Cloud assets (e.g., services, VMs, storage, networks)

- Applications (e.g., workloads or private clouds, web services, software as a
- service)

5. Understand and Apply Foundational Security Operations Concepts

- Need - to - know/least privilege (e.g., entitlement, aggregation, transitive trust)
- Separation of duties and responsibilities
- Monitor special privileges (e.g., operators, administrators)
- Job rotation
- Information lifecycle
- Service - level agreements

6. Employ Resource Protection Techniques

- Media management
- Hardware and software asset management

7. Conduct Incident Management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

8. Operate and Maintain Preventative Measures

- Firewalls
- Intrusion detection and prevention systems
- White listing/Blacklisting
- Third- party security services
- Sandboxing
- Honey pots/Honey nets
- Anti-malware

9. Implement and Support Patch and Vulnerability Management

10. Participate In and Understand Change Management Processes (e.g., Versioning, Base lining, Security Impact Analysis)

11. Implement Recovery Strategies

- Backup storage strategies (e.g., offsite storage, electronic vaulting, tape rotation)
- Recovery site strategies
- Multiple processing sites (e.g., operationally redundant systems)
- System resilience, high availability, quality of service, and fault tolerance

12. Implement Disaster Recovery Processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and awareness

13. Test Disaster Recovery Plans

- Read- through
- Walkthrough
- Simulation
- Parallel
- Full Interruption

14. Participate In Business Continuity Planning and Exercises

15. Implement and Manage Physical Security

- Perimeter (e.g., access control and monitoring)

- Internal security (e.g., escort requirements/visitor control, keys and locks)

16. Participate In Addressing Personnel Safety Concerns (E.G., Duress, Travel, Monitoring) [15]

[15] Cryptography podcasts

Domain 8

Software Development Security[16]

(Understanding, Applying, and Enforcing Software Security)

Overview

Security in software development is the last domain of the CISSP examination requirements. This domain lets you know the security controls that must be fulfilled while working in software development environments. You will be able to learn the security concepts that are currently in force for ensuring information security during the development and implementation of a software application. This tells us how best security practices must be adhered to and followed while going through the systematic development and launching of new software applications or while redeveloping the existing software solutions.

A CISSP professional is not expected to be a skilled software developer or a qualified software security engineer. But they must know how to assess the requirements necessary for implementing the right types of security controls. They must also know how to enforce the security boundaries for the safe and secure operation of the software application within the ambit of the overall information security system.

For the purpose of ensuring the right ways of implementing the security controls that are in place, the CISSP person must be able to know how to enforce the security guidelines during every phase of the software development lifecycle. To make sure that the CISSP candidates have sufficient knowledge for ensuring information security while working with software development scenarios, they will be tested for their level of knowledge in:

- Types and nature of software development methodologies
- Software maturity models
- Operations and maintenance of software development systems

[16] Videos on Software Development Security

- Providing for change of management during software development life cycle
- Providing for an integrated development team to take charge of each of the stages in the software development lifecycle

As a certified information security professional it is necessary to have knowledge in the concepts that deal with enforcement of security controls in all types of software development environments. For this you must have learnt the concepts that deal with anticipated security vulnerabilities in the software development process like

- Security consideration for software development tools
- Security issues that are likely to arise due to weakness in the software development methods currently in use
- Security related weaknesses in the source code
- Vulnerabilities in security set ups due to improper or wrong coding of the software applications
- Security concerns that arise during the configuration and setting up of the software application into the overall information security system
- Ensuring security in the code repositories
- Providing for the right type of security in respect of Application programming interfaces

Apart from these, the candidates for CISSP have to prove their depth of knowledge in the concepts relating to the software security control assessment. For this, you have to focus on the topics of logging and auditing with emphasis to change of management, analysis of risk and vulnerabilities and taking suitable mitigation activities for ensuring an enhanced level of software security. You also need to have good knowledge in the impact of the software applications that have been acquired from external sources.

> "CISSP'S ARE NOT, GENERALLY SPEAKING, SOFTWARE DEVELOPERS OR SOFTWARE SECURITY ENGINEERS; HOWEVER, IT IS INCUMBENT UPON THEM TO ASSESS AND ENFORCE SECURITY CONTROLS ON SOFTWARE BEING OPERATED WITHIN THEIR ENVIRONMENTS." *~CISSP HANDBOOK*

Key Areas of Knowledge

1. Understand and apply security in the software development lifecycle

The security of the information system depends on the level of security you have built into each component of the overall security system. As most of the sub-systems are software driven you have to understand the vulnerabilities inherent in each one of them. This will help you build a sound security system without compromising on the functional abilities of various software applications you are using.

Apart from this when you are developing a new software application for your information security system or for the use of your organization you must specify the security imperatives that must be built into the software. This will help the developers understand the level and type of security features you expect in the applications once they are launched and running. This is a better way to enhance the security behavior of the software development process than finding the vulnerabilities and addressing them later after the software application has been built and launched.

This calls for good knowledge of the software development lifecycle and the current methodology that is being used for creating the software. As the security requirements and degree of errors, Security holes and vulnerabilities change with the methodology used for the software development you must have more knowledge on these, especially the most modern Agile methodology or the more common and traditional waterfall methodology.

You should also acquire enough knowledge in the maturity models that are applicable to the software development cycles and their natural levels of security. When you find that there is need for more stringent security routines you have to specify the necessary security protocols that must be followed while developing and testing the maturity models so that the software applications abides by your security directions.

Once the software application was developed and launched you have to test the same against your set security values and satisfy yourself as to the compliance of all the security requirements you have asked for. While operating the application you may notice some vulnerability due to coding inefficiencies and you have to provide the right counter measures so that the software application does not pose any security issues to your information security system.

Towards this and to ensure that you understand the importance of acquiring knowledge for proper development of the software application with required security norms you have to study the following concepts in some detail:

- Development methodologies (e.g., Agile, Waterfall)
- Maturity models
- Operation and maintenance
- Change management
- Integrated product team (e.g., DevOps)

2. Enforce security controls in development environments

When you want to ensure confidentiality, availability and integrity of your information security system then you have to place the security controls right from the development stage. Developing a software application involves many persons and many processes. It is not possible to have a one on one control of the entire range of processes or users who are involved in developing the software application. Further to complicate your security control enforcement the development of the software application may take place at an off shore outsourced location over which you cannot enforce any sort of security routines.

To obviate the occurrence of any of the security issues that may crop up due to the flaws in the software development process you need to state, deliver and enforce the security controls even before the start of the software application. This is to ensure that the software application development process is carried with the full knowledge and commitment to the security routines you want to enforce in the software application.

An easy and effective way would be to select and involve a security enabled software development environment or make your software development environment a fully secure one. While proceeding with the software development you must stress the necessity for following a software development methodology that does not give any room for security weaknesses or unknown and unexpected vulnerabilities. This helps you access the types of security issues that may crop up during its operation and be ready with suitable counter measures to deal with them in such a way no serious security issues are seen in your information security system.

All software applications need configuration before they can be integrated into the system and begin their functioning. This is an important occasion for checking the security readiness of the software application. You have to device suitable routines and place the right protocols to check for any unanswered vulnerabilities and try to remove them at the first instance or be ready to counteract their effects once they are found to be the result of faults in the source code.

Hence it is necessary for the CISSP person to have good configuration management skills to make the software application run with all types of security controls right from the time of their configuration.

The other instances of security breach occur in the code repositories unless you are aware of the vulnerabilities in the coding of the software application. Providing security at the code repositories is the most reliable way of securing the software application development phase and its installation phase. This includes the necessity for providing the necessary amounts of security at the programming interfaces as they are the main sources of interaction with outside world hence they become easy targets of attacks.

Due to all these the CISSP curriculum lays special emphasis on how to enhance the security of the software application during its development phase and for this you must have sound working knowledge in the following concepts:

- Security of the software environments
- Security weaknesses and vulnerabilities at the source-code level (e.g., buffer
- Overflow, escalation of privilege, input/output validation)
- Configuration management as an aspect of secure coding
- Security of code repositories
- Security of application programming interfaces

3. Assess the effectiveness of software security

Effective security can be implemented only by constant assessing and monitoring of the security controls you have placed in the software development lifecycle. This is necessary and vital for the success of the overall information security system that is geared towards fulfilling the demand for a secure and safe working environment for the organization.

While ensuring the proper functioning of the security system, various types of audits are conducted to

- know the performance level of security controls
- the effectiveness of these controls as well as their preparedness to act on any vulnerabilities

the results of these audits helps you understand the security routines you have devised to safeguard your information security system and make it work as desired. Audits may be conducted through internal teams or through external agencies and they must be done in a periodical manner to get the desired results and to be prepared to meet any eventualities.

Software applications tend to change during their various phases of working life and these changes may bring about new vulnerabilities and weaknesses. You have to assess the effects of these changes on the security controls. Whenever a new change in the software application function is noticed then you have to look for its corresponding weakness or vulnerability prompting you to launch the necessary counter measures.

Risk analysis of various factors that are functioning as a part of your information security system is a vital function of the CISSP professional. To obviate the happening of any unexpected security issues, it is necessary to conduct risk analysis on every part of the software application development process and the resulting products. This will give a good handle over the selection and implementation of the right type of security controls for the software applications. Mitigation of the security issues that come to the notice during the risk analysis is to be done at the right time without delay or waiting for the security issue to arise.

Acceptance testing helps in finding the particular elements of the software application that readily accepts your demands of various security controls you want to be implemented into the system. To know the acceptance level of the system in question you must know how to do an acceptance testing and based on its results, you must be able to put in additional security controls or modify the existing ones that are not showing good acceptance and implement them to ensure the required level of security.

Towards this focus on the following concepts while preparing for your CISSP certification namely:

- Auditing and logging of changes
- Risk analysis and mitigation
- Acceptance testing

4. Assess Security Impact Of Acquired Software

In the day to day functioning of the organization it is necessary to use many software applications that are developed by third parties. These applications may not be having all the security elements put into them during their development. When your organization wants to use them for its purposes, you need to conduct a security assessment of the acquired software. This will help you find the level of security available in the application and if it is not up to your expected level you have to add the necessary security controls to it to make it comply with your security requirements.

If this is not possible then you have to find the security impact of the acquired software application by carefully studying its known vulnerabilities and fine tune your security controls to take care of these vulnerabilities. You must be prepared not only to face any type of threats that are known now but also expect during its operation at later stages.

Hence your ability to assess the security impact of the acquired software is a necessary feature you must be well prepared to ensure the confidentiality, integrity and availability of information at all times.[17]

[17] Podcast episodes for Domain 8

References:

Arata, A. (2005). *Perimeter Security.*

Bacik, S. (2008). *Building an Effective Information Security Policy Architecture.*

Bertino, E, Takahashi (2011). *Identity Management: Concepts, Technologies, and Systems.*

Bosworth, S, Kabay, M, Whyne E (2009). *Computer Security Handbook.*

Boudriga, N. (2009). *Security of Mobile Communications.*

Buffington, J (2010). *Data Protection for Virtual Data Centers.*

Chin, S, Older, S (2010). *Access Control, Security and Trust: A Logical Approach.*

Davis, C (2001). IPSec: *Securing VPNs.*

Dowd, M, McDonald J, Schuh (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities.*

Dwivedi, H (2010). *Mobile Application Security.*

Fennelly, L (2012). *Effective Physical Security.*

Foreman, P (2009). *Vulnerability Management.*

Hernandez, S. (2012). *Official (ISC)2 Guide to the CISSP CBK (3rd edition).*

Herold, R. (2010). *Managing an Information Security and Privacy Awareness and Training Program, (2nd edition).*

Kadrich, M (2007). *Endpoint Security.*

Kenan, K (2005). *Cryptography in the Database: The Last Line of Defense*

Khairallah, M (2005. *Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems.*

Landoll, D. (2011). *The Security Risk Assessment Handbook: Complete Guide for Performing Security Risk Assessments.*

Luotonen, A (1997). *Web Proxy Servers.*

Newman, R (2009). *Security and Access Control Using Biometric Technologies: Application, Technology, and Management.*

Nissenbaum, H (2009). *Privacy in Context: Technology, Policy and the Integrity of Social Life.*

Prowell, S, Kraus, R, Borkin (2010). *Seven Deadliest Network Attacks.*

Rajnovic, D (2010). *Computer Incident Response and Product Security.*

Santos, O. (2007). *End-to-End Network Security: Defense-in-Depth*

Stallings, (2013). *Cryptography and Network Security: Principles and Practice, 6th edition.*

Swidersky, F, Snyder, W (2004). *Threat Modeling.*