UNIT I

PLANNING FOR CYBER SECURITY

SECURITY MANAGEMENT FUNCTION

Security Function:

Security function is a major requirement for every organization and must knowledge for those preparing for CISSP Certification exam. Anyone looking forward towards attaining a CISSP certification needs to realize the best practices on managing the security function. Let's discuss the same in this post.

- **Budget and Resources for Information Security Activities:** The security officer must work with the application development managers to ensure that security is considered in the project cost during each phase of development.
- **Evaluate Security Incidents and Response:** Periodic compliance, whether through internal or external inspection, ensures that the procedures, checklists, and baselines are documented and practiced. Compliance reviews are also necessary to ensure that end users and technical staff are trained and have read the security policies.
- **Establish Security Metrics:** Various decisions need to be made when collecting metrics, such as who will collect the metrics, what statistics will be collected, when they will be collected, and what are the thresholds where variations are out of bounds and should be acted upon.
- **Participate in Management Meetings:** Security officers must be involved in the management teams and planning meetings of the organization to be fully effective.
- **Ensure Compliance with Government and Industry Regulations:** Governments pass new laws, rules, and regulations that establish requirements to protect nonpublic information or improve controls over critical processes with which the enterprise must be in compliance.
- **Develop and implement information security strategies:** Information security consultants, both technology and process oriented, play pivotal roles in developing and implementing the organizational security and practices.

- **Assist Internal and External Auditors:** Assist Internal and External Auditors for assessing the completeness and effectiveness of the security program.
- **Stay Abreast of Emerging Technologies:** The security officer must stay abreast of emerging technologies to ensure that the appropriate solutions are in place for the company based upon its risk profile, corporate culture, resources available, and desire to be an innovator.
- **Maintain Awareness of Emerging Threats and Vulnerabilities:** The threat environment is constantly changing and the security office needs to be aware of each and every change.
- **Understand Business Objectives:** This understanding increases the chances of success, allowing security to be introduced at the correct times during the project life cycle.
- **Security Awareness Program:** The security officer provides the leadership for the information security awareness program by ensuring that the program is delivered in a meaningful, understandable way to the intended audience.

Information security Management Function:

ISO 27001

ISO-27001 is part of a set of standards developed to handle information security: ISO 27001 was developed to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).

Importance of ISO 27001:

The standard provide companies with the necessary know-how for protecting their most valuable information in this way, prove to its customers and partners that it safeguards their data.
What are the 3 ISMS security objectives?
The basic goal of ISO 27001 is to protect three aspects of information:

- Confidentiality: only the authorized persons have the right to access information.
- Integrity: only the authorized persons can change the information.
- Availability: the information must be accessible to authorized persons whenever it is needed

What is an ISMS?

An Information Security Management System (ISMS) is a set of rules that a company needs to establish in order to:

1. identify stakeholders and their expectations of the company in terms of information security
2. identify which risks exist for the information
3. define controls (safeguards) and other mitigation methods to meet the identified expectations and handle risks
4. set clear objectives on what needs to be achieved with information security
5. implement all the controls and other risk treatment methods
6. continuously measure if the implemented controls perform as expected
7. make continuous improvement to make the whole ISMS work better
8. There are four essential business benefits that a company can achieve with the implementation of this information security standard:
9. Comply with legal requirements

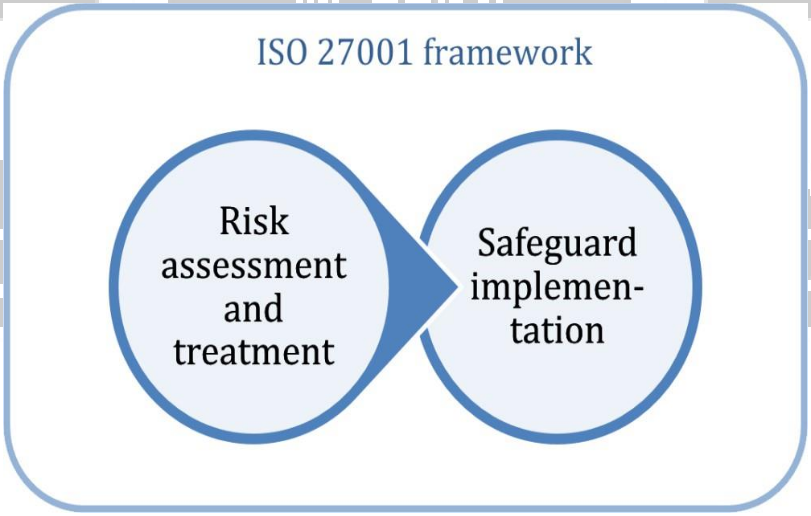
– there is an ever-increasing number of laws, regulations, and contractual requirements related to information security, and the good news is that most of them can be resolved by implementing ISO 27001 – this standard gives you the perfect methodology to comply with them all.

10. Achieve competitive advantage – if your company gets certified and your competitors do not, you may have an advantage over them in the eyes of those customers who are sensitive about keeping their information safe.

11. Lower costs – the main philosophy of ISO 27001 is to prevent security incidents from happening – and every incident, large or small, costs money. Therefore, by preventing them, your company will save quite a lot of money. And the best thing of all – investment in ISO 27001 is far smaller than the cost savings you'll achieve.

12. Better organization – typically, fast-growing companies don't have the time to stop and define their processes and procedures – as a consequence, very often the employees do not know what needs to be done, when, and by whom. Implementation of ISO 27001 helps resolve such situations, because it encourages companies to write down their main processes (even those that are not security-related), enabling them to reduce lost time by their employees.

How does ISO 27001 work?


ISO 27001 framework
Risk assessment and treatment
Safeguard implemen-tation