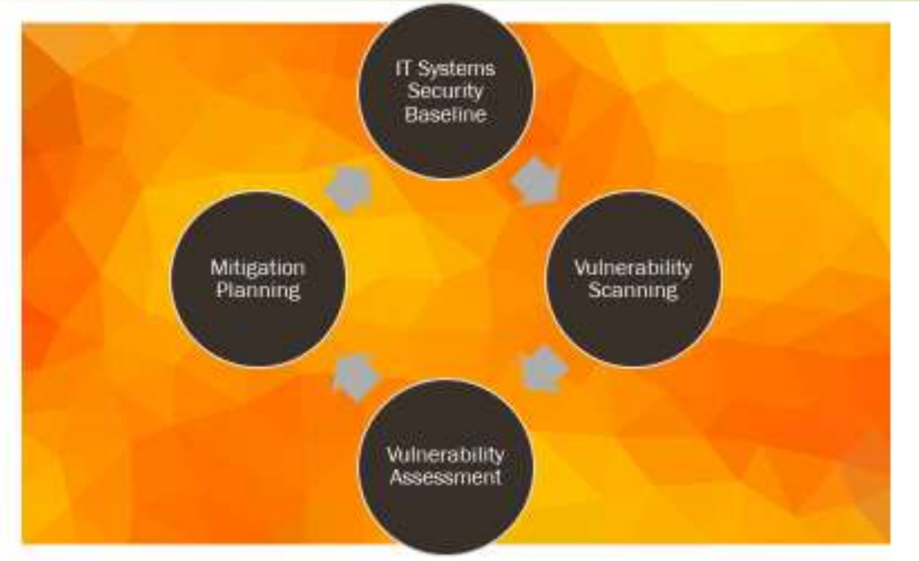
Task-3

Virtual Case Experience

Cyber Security

IT Systems Security Baseline

- The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. A set of information security controls that has been established through information security strategic planning activities to address one or more specified security categorizations; this set of security controls is intended to be the initial security control set selected for a specific system once that system's security categorization is determined.
- Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them. This is an integral component of a vulnerability management program, which has one overarching goal – to protect the organization from breaches and the exposure of sensitive data.
- A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.
- The mitigation plan outlines the planning process for identifying and implementing actions to reduce or eliminate business losses, loss of life, property, functions, etc. due to any type of hazards.



Why an up-to-date Information System Security Baseline is crucial?

- Before you can recognize abnormal system behavior as a sign of attack, you need to know what normal behavior is. In other words, you need a security baseline. In setting a baseline, it is important to harden or lock down your servers and networks at a level where incursions are less likely to occur. These would introduce you to the concepts of operating system, network, and application hardening making it more secure.