Pre-investigation Phase

Steps Involved in the Pre-investigation Phase

Set Up a Computer Forensics Lab	A computer forensics lab (CFL) is a designated location for conducting computer-based investigation of the collected evidence in order to solve the case and find the culprit
Build the Investigation Team	The team is responsible for evaluating the crime, evidence, and criminals
Review Policies and Laws	Identify possible concerns related to applicable federal statutes, state statutes, and local policies and laws
Establish Quality Assurance Processes	Establish and follow a well-documented systematic process for investigating a case that ensures quality assurance
Data Destruction Industry Standards	Destruction of data using industry standard data destruction methods is essential for sensitive data that one does not want falling into the wrong hands
Risk Assessment	Risk assessment is useful to understand information security issues in a business context and to assess their impact on the business

Investigation Phase

Steps involved in the Investigation Phase

Initiate the Investigation Process	Incident responders should have a clear idea about the goals of the examination prior to conducting the investigation
Perform Computer Forensics Investigation	1 First Response 2 Search and Seizure 3 Collect the Evidence 4 Secure the Evidence 5 Data Acquisition 6 Data Analysis

Notes:

Post-investigation Phase

Steps involved in the Post-investigation Phase

Evidence Assessment	The process of relating the obtained **evidential data** to the incident for understanding how the complete incident took place
Documentation and Reporting	The process of **writing down all actions** the incident responders performed during the investigation to obtain the desired results
Testify as an Expert Witness	The members who are present in a court of law may be unaware of the technical knowledge regarding the crime, evidence, and losses, so the investigators should approach authorized personnel who can appear in court to affirm the accuracy of the process and the data

LO#13: Explain Software Development Security

Notes: _____