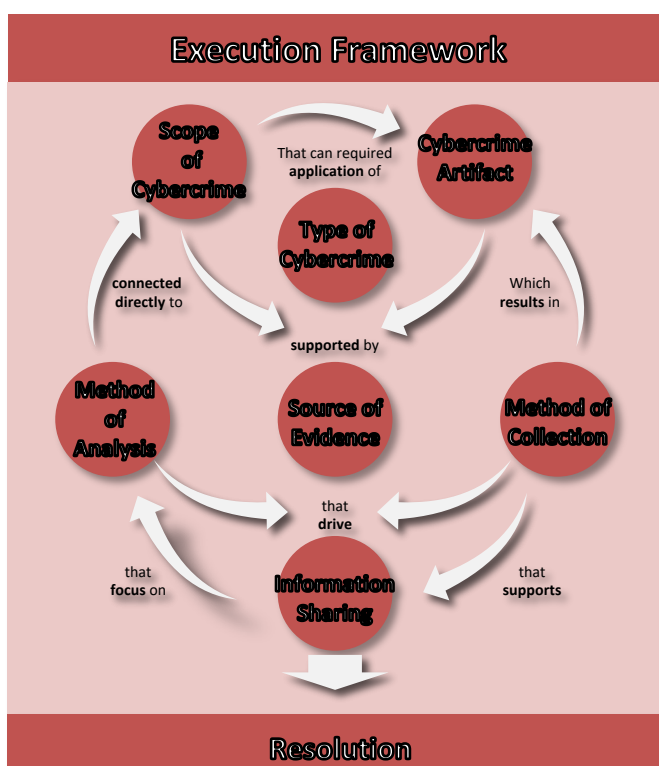# Cybercrime Investigation Body Of Knowledge

## Fundamental Training Course

## *Overview*

 Upon conducting an investigation of cybercrime which is continuously evolving , this course is aimed to enable law enforcement agency or cybercrime investigations team  to deal with incidents correctly and systematically in their respective positions. By using  common framework you can understand knowledge and its essence needed for that and through this training, you will learn the outline of various areas related to Cybercrime effectively .

## *A framework in CIBOK*



 This framework shows the eight elements and the correlation necessary in order to proceed the process of cybercrime investigation correctly. By understanding each element, you can learn the knowledge area and its essence that are necessary in the process of cybercrime investigation effectively.

# Learning Goals

- To be able to understand knowledge area and its essence that are necessary in the process of cybercrime investigation.
- To be able to grasp the gap with your knowledge and  devise a continuous and effective learning plan.
- To be able to carry out an assessment, re-evaluation, and improvement instructions of ability to investigate cybercrime in your organization.
- To be able to understand a proper cooperation way of Law enforcement agencies and victims' organizations and  also device a plan for improvement of current process.

# Topics（2-day course）

◆ CIBOK Chapter 1 & 2 Cybercrime and its investigation, Types of Cybercrime
  - Defining Cybercrimes
  - Types of cybercrimes including their objectives and motivations
◆ CIBOK Chapter 3 & 4 Artifacts of cybercrime, Scope of cybercrime
  - External/Internal artifacts and IOC of cybercrime
  - Nature and risk of cybercrime
◆ CIBOK Chapter 5 & 6 Source of Evidence , Method of Evidence collection
  - External/internal source of evidence
  -  Procedure and tools to collect evidence
◆ CIBOK Chapter 7 Methods of Evidence Analysis
  - Analysis framework  of evidence
◆ CIBOK Chapter 8 Resolution
  -  Resolution in Cybercrime
  - Organization, communication, tools and procedure required for final processing
◆ CIBOK Chapter 9 Cybercrime information sharing
  - What cybercrime information sharing is
  - Information sharing method and legal notes

# Who should take this course

- Investigators  in departments related to cyber security
- Investigators in law enforcement agencies

# Prerequisites

-  Those who can perform basic operation of Windows, or have equivalent knowledge.
   *Detailed technical knowledge is not necessary in this course . We recommend that you have basic knowledge of network and information security.