Cybercrime Investigation Body of Knowledge

# Training Courses

## Training for Skill/Knowledge development for cybercrime investigation

This training is designed to master overview of knowledge, skill and technique for cybercrime investigation such as how to identify, respond, and investigate cybercrimes, which is required by law enforcement and corporate security officers and executives.

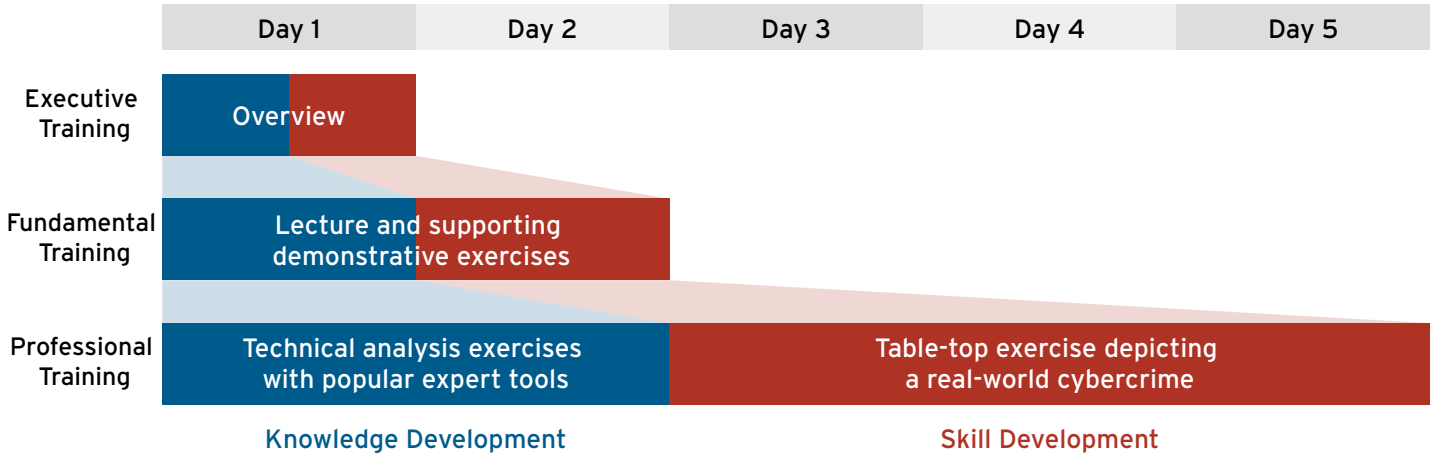
### Who should take a course!

Law enforcement investigators and prosecutors, and corporate auditors and incident handlers who may be tasked with related risk and compliance assessments and mitigation.

## Training Course Objectives

- Promoting a commonsense approach concerning consistent international cybercrime investigations, without dependency of laws of each country.
- Detailed demonstration of the positioning of other systematized customary practices, project management, computer science and digital forensics.
- To provide a framework for developing training curricula and individual knowledge and skills pertaining to duties of investigators and responders.
- Characterizing and demonstrating the content that should be put into practice in cybercrime investigations.
- Presenting means to utilize the topics covered in this body of knowledge of cybercrime investigations collected from experienced professionals.

## Training Level and Duration




For more details: www.cibok.org
Contact: secretariat@cibok.org

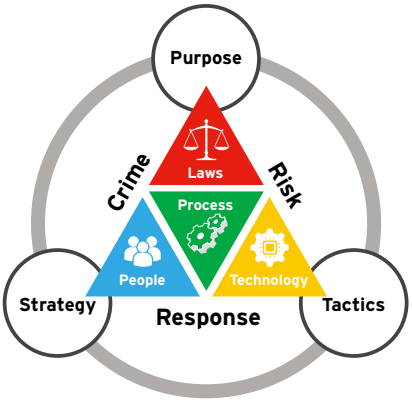
Cybercrime Investigation Body of Knowledge

# Training Courses

## Executive Training Course

**5 hours high level introduction for knowledge and skill**

| | |
|---|---|
| Introduction to CIBOK<br>Cybercrime and its Investigation<br>Types of Cybercrimes<br>Artifacts of Cybercrime<br>Scope of Cybercrime<br>Sources of Evidence<br>Methods of Evidence Collection<br>Methods of Evidence Analysis<br>Incident Resolution<br>Cybercrime Information Sharing<br>Management Framework | High level introduction for the task with related risk and compliance assessments and mitigation, including Q&A session |




## Fundamental Training Course

**Day 1: Knowledge Development**

| | |
|---|---|
| The 5 objectives of CIBOK<br>What is a Cybercrime?<br>What are Cybercrime Investigations?<br>What are challenges to Cybercrime Investigations?<br>What skills, knowledge and experience are necessary to develop investigative capabilities? | • To include jurisdictional considerations and information sharing within international privacy boundaries. |

**Day 2: Skills Development**

| | |
|---|---|
| What is "evidence" vs. "artifacts" of cybercrime?<br>What are the sources of evidence?<br>What are the methods of evidence collection?<br>How should evidence be handled for investigative and judicial purposes?<br>What are methods of analysis for evidence of Cybercrimes?<br>What sources of information are available to intelligently discover or prevent Cybercrimes?<br>How should information about Cybercrimes be shared?<br>What are the minimum organizational requirements for a Cybercrimes investigation unit?<br>What tools and training are available to develop Cybercrimes investigation staff? | • The identification (and discretion) of crimes versus anomalous activities, and methods of evidence collection and handling – for analysis.<br>• Methods of efficient collection, processing and analysis with popular expert tools.<br>• Limited technical demonstrations for discussion. |

## Professional Training Course

**Day 1-2: Knowledge Development**

| | |
|---|---|
| The 5 objectives of CIBOK<br>What is a Cybercrime?<br>What are Cybercrime Investigations?<br>What are challenges to Cybercrime Investigations?<br>What skills, knowledge and experience are necessary to develop investigative capabilities? | • Retail/POS Breaches<br>• Tech/Defense IP Theft<br>• Healthcare/Gov Data Theft<br>• Bank ATM/Payments Network Theft<br>• Social networks/services identity theft and Fraud |

**Day 3-5: Skills Development**

| | |
|---|---|
| What is "evidence" vs. "artifacts" of cybercrime?<br>What are the sources of evidence?<br>What are the methods of evidence collection?<br>How should evidence be handled for investigative and judicial purposes?<br>What are methods of analysis for evidence of Cybercrimes?<br>What sources of information are available to intelligently discover or prevent Cybercrimes?<br>How should information about Cybercrimes be shared?<br>What are the minimum organizational requirements for a Cybercrimes investigation unit? | • The identification (and discretion) of crimes versus anomalous activities, and methods of evidence collection and handling – for analysis.<br>• Methods of efficient collection, processing and analysis with popular expert tools.<br>• Technical demonstrations, with associated exercises and samples. |

For more details: www.cibok.org

Contact: secretariat@cibok.org