

Training course “Fraud prevention in IT systems”

Version: 2021-07-06

Author: Glib Pakharenko

Duration: 2 days

The “Fraud prevention in IT systems” training allows participants to gain a wide set of knowledge to detect, respond and investigate fraud cases. They will gain all required skills to face the most difficult problems, which include:

- investigation complex fraud cases
- building system of fraud controls
- evaluating effectiveness of the fraud controls.

This is solely practical training! The participants immediately will work. The training is adapted for an audience which represents students with completely different background. If you are just a novice, you will be solving simple tasks. If you are professional, you will have a set of very sophisticated tasks. The obtained experience will mandatorily increase your value for employees and customers and bring a tremendous level of a professional confidence to you personally.

The training course is designed for:

- internal auditors
- security specialists
- anti-fraud specialists.

Course syllabus: “Fraud prevention in IT systems”

1. Introduction

- 1.1. Types of fraud
- 1.2. Opportunity, Pressure/Incentive, Rationalization
- 1.3. Who is fraudster?
- 1.4. Law related to fraud
- 1.5. Individual rights during examinations
- 1.6. Warm-up fraud cases

2. Fraud prevention

- 2.1. 4 hands rule
- 2.2. Chinese walls
- 2.3. Internal whistleblowing
- 2.4. Job rotations
- 2.5. Mandatory vacations
- 2.6. Screening
- 2.7. Exit interviews
- 2.8. Data analysis
- 2.9. Symptoms of fraud

3. Fraud investigation and reporting

- 3.1. Investigating theft
- 3.2. Analysing documents
- 3.3. Conversion methods
- 3.4. Covert examinations
- 3.5. Inquiry methods
- 3.6. Basic digital forensics
- 3.7. Basic principles of evidence
- 3.8. Management level fraud
- 3.9. Fraud in E-commerce
- 3.10. Electronic payment tampering
- 3.11. Theft of intellectual property
- 3.12. Financial statement fraud and role of IT systems
- 3.13. ATM fraudster

This syllabus can be modified according to the needs of the company/organisation.

- 3.14. Credit card fraud
- 3.15. Resolution of fraud
- 3.16. Report writing

4. IT general controls

- 4.1. Logical access controls over infrastructure, applications, and data
- 4.2. System development life cycle controls.
- 4.3. Program change management controls.
- 4.4. Physical security controls over the data centre
- 4.5. System and data backup and recovery controls
- 4.6. Computer operation controls

5. Application controls

- 5.1. Input controls
- 5.2. Output controls
- 5.3. Processing controls.