

# Syllabus

**Title:** Forensic Readiness

**Duration:** 1 day (9:00 – 5:30). Lunch will be provided.

**Frequency:** Monthly. Additional courses will be provided to meet demand and courses can be run for individual companies.

**Who should attend:** Managers or department heads, auditors or HR personnel and other employees who do not necessarily come from an IT background but may need to understand the implications of an investigation.

**Number of Delegates:** The maximum is 6 delegates to ensure personal attention is given to every delegate by the tutor.

## Overview:

The aim of this course is to provide delegates with a foundation in the concepts related to a forensic investigation, the preservation and processing of computer evidence.

The intention is that after the course the delegate will be fully aware of the basic principles of computer forensics. The delegate will be able to appreciate the different facilities available to him/her and will have enough knowledge to know how **not** to corrupt any future investigation.

The delegate will gain a much better understanding of the full forensic process including Association of Chief Police Officers (ACPO) principals, current laws and legislation. The delegate will also learn how to adapt its internal company policies to be more relevant to today's world when using recognised forensic tools and methods.

A full copy of the presentation slides will be issued upon completion of the course to every delegate.

## Agenda will cover:

Digital Evidence	Surveillance and Access
Investigations	Computer Misuse Act
Incident Timeline	Material Types
Evidence Sources	Search and Seizure
Evidence Types	Disclosure and Procedures
Incident Management	Forensic Tools
Internal Handling and Resource	Good Practice Guide
Forensic Process	

Note: It is important to understand that this course does not provide attendees with certified training certificates in any of the products discussed.

