Computer Law/Policy Terminology

Terminology	Details
ACPO	**Association of Chief Police Officers** There are 4 main principles of the ACPO Good Practice Guide for Computer Based Electronic Evidence
Attack Vector	A path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome
Chain of custody	Chronological documentation (or paper trail) that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
Computer Misuse Act 1990	Law that deals specifically with the crime of accessing or modifying data stored on a computer system without being authorised to do so.
Evidence Integrity	The validity of information. derived from examination of the physical evidence depends entirely upon the care with which the evidence has been protected from contamination.
GDPR	**General Data Protection Regulation**
Personal data - GDPR	Personal data are any information which are related to an identified or identifiable natural person.
Regulation of Investigatory Powers Act 2000	Regulating the powers of public bodies to carry out surveillance, investigation and covering the interception of communications.
RTO	**Recovery Time Objective** For Disaster recovery situations
Safe Harbour Agreement	A set of principles that governed the exchange of data between the USA and the EU. Ruled invalid in 2015. Led to the creation of the EU-US Privacy Shield.
Timestomping	A technique that modifies the timestamps of a file created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools.
Vulnerability	A weakness in an IT system that can be exploited by an attacker to deliver a successful attack.
IETF	**Internet Engineering Task Force**
Risk Assessment	Overall process or method where you: Identify hazards and risk factors that have the potential to cause harm (hazard identification). Analyze and evaluate the risk associated with that hazard. **Risk Assessment Aspects: Impact, Likelihood, Cost**
Penetration Testing	A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.