Seminar session 7: Principles of Digital Forensics and Cyber Law – Digital forensic expert evidence standards and Case Study Review

Activity 1: ISO/IEC 27043:2015

- ISO (the international Organisation for Standardisation) and IEC (the International Electrotechnical Commission) established a system for worldwide standardisation
- National bodies that are members of ISO or IEC involve in development of International Standards
- ISO/IEC technical committees collaborate in the field of mutual interest
- Other international organizations, governmental and non-governmental also take part in the work

- This standards provides guidelines for common investigation processes during various investigation scenarios
- It includes process from pre-incident preparation, returning evidence for storage or dissemination, general advice, appropriate identification, collection, acquisition, preservation, analysis, interpretation and presentation of evidence
- The basic principle of digital investigation is repeatability where a skill investigator required to obtain same results as other investigators

Guidelines for digital investigation:

- Guidelines would expedite the investigation process
- It provides common order of events that an investigation required
- It allow smooth transition from one event to another during the investigation
- These guidelines also allow proper training of inexperienced investigators
- It also ensures flexibilities within an investigation
- Harmonised investigation process model should be used in criminal and civil prosecution settings
- Any digital investigation requires high level of expertise, those involved in investigations, have to be competent, proficient and they need to use validate processes, such as ISO/IEC 27041

What is the digital forensic standard of reporting?

- ISO describes the comprehensive investigative process that includes:
  ➔ Incident management (preparation and planning for investigation)
  ➔ Handing of digital evidence
  ➔ Use of redaction (process of editing text for publication)

- ➔ Intrusion prevention and detection system
- ➔ Security of storage
- ➔ Ensuring that investigative methods are fit for purpose
- ➔ Carrying out analysis and interpretation of digital evidence
- ➔ Understanding principles and processes of digital evidence investigations
- ➔ Security incident event management
- ➔ Relationship between electronic discovery and other investigations
- ➔ Governance of investigations