GAQM®
Global Association for Quality Management

Exam Name - Certified Forensic Analyst (CFA)™

Exam Code – CFA-001

<u>Sample Exam</u>

(Question): Which of the following are typical investigation reasons that may warrant an investigation? (Choose three)

(A): Theft of information
(B): Electronic tampering
(C): Internet speed issue
(D): Intellectual property infractions
(E): Physical assault

(Correct): A,B,D

(Question): Which of the following activities are involved in Electronic Tampering? (choose three)

(A): Masquerading
(B): Spoofing
(C): Property infraction
(D): Auditing
(E): Masking

(Correct): A,B,E

(Question): True or False: Before performing any investigation on e-mail, you need to ensure that corporate policy allows it.

(A): True
(B): False

(Correct): A

© Global Association for Quality Management (GAQM)

(Question): Baselines that guide many complaints (or a justification to investigate) often include misuse or violation of: (Choose three)

(A): Company policies and procedures
(B): Standard operating procedures
(C): Mandatory statues
(D): Regulatory statues

(Correct): A,C,D

(Question): Who should a forensic investigator contact for policies and procedures, employee information and complaint reports?

(A): Internal auditor
(B): Legal department
(C): Human resources
(D): External consultant

(Correct): C

(Question): Who should a forensic investigator contact for policies and procedures, after-hours logs to work areas, security camera tapes, key card access logs and incident reports.

(A): Legal department
(B): External consultants
(C): Information security department
(D): Physical security department

(Correct): D

(Question): Which of the following should an investigator do to conduct an effective investigation? (Choose three)

(A): Available resources
(B): Authority
(C): Reporting hierarchy
(D): Scalability report

(Correct): A,B,C

(Question): Which of the following is required by an Investigator to track web sites that have been visited by an employee? (Choose three)

(A): Cookies
(B): History buffer
(C): Cache
(D): Downloads
(E): Tools

(Correct): A,B,C

(Question): True or False: The name cookie evolved from UNIX objects called magic cookies.
(A): True
(B): False

(Correct): A