

**2ND SEMESTER 2021/2022 ACADEMIC YEAR**

**END OF SEMESTER EXAMINATION ANSWER BOOKLET**

THE FOLLOWING DETAILS MUST BE COMPLETED BY THE STUDENT

400

ADS19A00110Y

STUDENT’S ID NUMBER­­­­­­­­­­: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ LEVEL: \_\_\_\_\_\_\_\_\_\_

IT454

COMPUTER FORENSICS

COURSE COD**E: \_\_\_\_\_\_\_\_\_** COURSE TITLE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EMMANUEL ADOTEY PAPPOE

LECTURER’S NAME: (Refer to the Question Paper) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**QUESTION NUMBER: (e.g., Q1) \_\_1\_\_SUB-QUESTION (e.g., 1(a)) \_\_1A, B, C, \_**

1. The seven essential reviews that an IS auditor should undertake are;

* Check the test plan to make sure it is thorough; mention instances where users participated, such as when they created test scenarios or approved results; and think about running important tests again.
* Match up converted data with control totals.
* Examine error reports to see how well incorrect data is identified and corrected.
* Check the cyclical processing for accuracy (month-end, year-end processing.).
* Confirm the accuracy of important output and reports utilized by management and other stakeholders.
* Speak with system end users to assess their comprehension of new techniques, processes, and operational guidelines.
* Examine system and end-user documentation to ascertain its accuracy and confirm its completeness during the testing phase.

1. The chain of custody can be utilized to verify the reliability of evidence that has been submitted in court as well as to demonstrate the transfer of ownership of digital evidence between different entities.

The rules that must be followed during the chain of custody process include:

* Data collection: Data must be identified, recorded, labeled, and acquired from all pertinent sources during the first stage of the investigation in order to maintain the validity of the evidence gathered.
* Examination: During this procedure, the chain of custody is recorded and it describes the forensic procedures used. Throughout the procedure, screenshots must be taken to document the tasks that are accomplished and the evidence that has been found.
* Analysis: This is the outcome of the examination stage. In order to gather relevant data for answering the questions raised in a certain case, legally acceptable procedures and techniques are used.
* Report: The chain of custody statement, a description of the tools used, a description of the analysis of the various data sources, the identification of problems and vulnerabilities, and suggestions for additional forensics measures are all included in the reporting stage.

1. The differences explained;

* Personal ethics pertains to a person's personal principles and standards of behavior. From the early beginning, parents, relatives, and friends implant these morals in the individual. The life of a person is brief and lacking without personal ethics. An individual's integrity, openness, accountability, and other traits, for instance, can be taken into account.
* Computer ethics are a collection of moral principles that guide how computers should be used. It is how the general public feels about using computers, both software and hardware.
* In a professional, a person's behavior reveals their personal ethics. A person's values and principles that are introduced to them in a professional organization are what is meant by professional ethics. Every employee in a corporation is obligated to abide by certain standards and cannot opt out of doing so. The professional world has to adopt these standards since they bring in a maintain the etiquette in the workplace and instill a feeling of discipline in the individual's life. Transparency, confidentiality, impartiality, and other principles are examples of professional ethics.

**QUESTION NUMBER: (e.g., Q1) \_\_3\_\_SUB-QUESTION (e.g., 1(a)) \_\_3A, B, C\_**

1. They are;

* Personal ethics pertains to a person's personal principles and standards of behavior. From the early beginning, parents, relatives, and friends implant these morals in the individual. The life of a person is brief and lacking without personal ethics. An individual's integrity, openness, accountability, and other traits, for instance, can be taken into account. These are moral principles that people generally apply to their behavior. An illustration of personal ethics is having regard and concern for others welfare.
* Impartiality and Objectivity: One of the most crucial aspects of doing an inquiry is coming to factual findings that are supported by solid evidence. When the issue is known to or familiar to the practitioner, it is up to them to maintain the highest level of objectivity throughout the course of the investigation in order to develop conclusions based on factual and reliable evidence.
* Professional ethics: Every employee in a corporation is obligated to abide by certain standards and cannot opt out of doing so. The professional world has to adopt these standards since they bring in a maintain the etiquette in the workplace and instill a feeling of discipline in the individual's life. Transparency, confidentiality, impartiality, and other principles are examples of professional ethics. It Concerns an individual or people who do a particular task, like digital forensics, in a professional ethics loyalty to one's obligations as a professional is one example.
* Diligence and duty of care: To minimize potential repercussions, informed decisions throughout an investigation must be taken in accordance with the relevant laws, rules, and standards. An expert must consistently display their behavior and Its conduct is carried out honestly, in accordance with the law, and industry standards.
* Computer Ethics: a collection of moral principles that guide how computers should be used. It is how the general public feels about using computers, both software and hardware. A set of guidelines and instructions for using computers ethically. As an illustration, consider how society sees the use of computers both the hardware and software.
* Business ethics is the application of the broad guidelines that were previously covered to conduct in a professional setting. An illustration might be: to safeguard the interests of individuals, the general corporate community, and the public interest.
* Openness and Disclosure: When examining the evidence, practitioners may come across some facts that require additional evaluation before factual conclusions can be drawn, such as paying attention to incriminating or conclusive evidence.
* Confidentiality and Trust: A great level of trust is placed in the work of a digital forensic specialist. They may appear extremely sensitive and privileged information that should only be shared with those who need to know it.

1. Ethics describes the moral standards that guide actions and judgments within an organization. In computer forensics, ethics refers to a set of moral standards that govern how workers should act or behave.

its importance in an organization;

* Builds a Positive Corporate Culture: An organization creates a positive corporate culture when it invests resources in creating policies and procedures that promote ethical behavior. When staff members believe they are safe from being punished for their personal opinions, team morale increases. These regulations include ones that prohibit discrimination, have open doors, and provide equal possibilities for advancement. Positive attitudes are more prevalent throughout a company when workers enjoy their jobs. As a result, employees are more loyal to the company and productive since they enjoy coming to work.
* Decision-Making: Making decisions based on ethics is encouraged by ethical behavior at work. Additionally, it increases transparency and responsibility while making any corporate decisions. When things are unstable, having a strong ethical culture helps you handle problems by acting in the correct ways. It can assist you in successfully implementing change within the organization, which can be difficult. You and your personnel become more aware of how to behave consistently even in difficult conditions as a result of your company's ethical behavior.
* Satisfying Basic Human Needs: One of the basic human needs is to be fair, honest, and ethical. Every employee aspires to be such themselves and to work for an organization that upholds moral principles.

1. The five basic standards that IS auditors are required to conform;

* Encourage adherence to relevant standards and guidelines for the efficient administration and management of business information systems and technology and support their implementation, including management of risk, controls, security, and audit.
* Carry out their responsibilities with objectivity, attention, and care, conformity with accepted practices.
* Act legally and ethically in the stakeholders' best interests while upholding high moral and ethical standards, not undermining their vocation, the Association, etc.
* Maintain the security and privacy of the data gathered through the they engage in, unless disclosure is mandated by a court of law.
* Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.

**QUESTION NUMBER: (e.g., Q1) \_\_4\_\_SUB-QUESTION (e.g., 1(a)) \_\_4A, B, C\_**

1. When shooting video or taking photographs to document a crime scene, best practices include:

* Providing a full view of the physical environment, including floor-to-ceiling and wall-to-wall.
* Capturing individual perspectives of dedicated work areas (as needed), such as cabinets, shelves, garbage cans
* Displaying connectivity between computer systems and external devices or any other devices, such as printers or switches
* It is critical not to press any keys or buttons that could cause the system to perform some action (i.e., logic bomb4).

Details about the crime scene must be documented in addition to photographs and videos. A committed note pad, or logbook, ought to be utilized by each computerized measurable expert for the purpose of keeping a precise record of occasions, action taken, and associations including their examinations. Like how policing report their cooperation in a logbook, legal practitioners need to record their endeavors on the assumption that the examination could ultimately wind up in court.

1. The following components are typically found in an information security governance framework:

* A comprehensive security plan that is inextricably tied to business objectives
* A complete set of standards for each policy to guarantee that procedures and guidelines comply with policy;
* Governing security policies that address every aspect of strategy, controls, and regulation Institutionalized monitoring procedures to ensure compliance and provide feedback on effectiveness.
* An efficient security organizational structure free of conflicts of interest.

This framework serves as the foundation for creating a cost-effective information security program that advances the organization's corporate objectives. The goal of the information security program is to create a set of procedures that ensures that information assets are protected to the extent necessary given their value or the danger that their compromise poses to the organization.

1. Examining the principles;

* Carefully reviewing and analyzing the evidence in a case.
* Conducting examinations based on recognized, validated standards.
* You must never give false information about your credentials, training, experience, or membership status.
* Give opinions with a basis that can be proven to be reasonable.
* Not suppressing any information that could lead to a misrepresentation of the facts of a case, whether it be incriminatory or exculpatory.

**PART B**

**QUESTION NUMBER: (e.g., Q2) \_\_1\_\_\_SUB-QUESTION (e.g., 2(a)) \_\_1A, B, C\_**

1. The six Issues to consider include:

Ease of use for existing and future audit staff

Training requirements

Complexity of coding and maintenance

Flexibility of uses

Installation requirements

Processing efficiencies

1. Importance of implementing an effective information security governance:

Information security governance has reached one of the highest levels of focused activity with specific value drivers due to its prominent position within IT governance processes, including confidentiality, integrity, and availability of information; service continuity; and protection of information assets. Global networking, rapid technical innovation and development, growing reliance on IT, growing sophistication of threat agents and exploits, and an expansion of the company beyond its conventional borders have all contributed to security being a serious governance concern. Information security is therefore a crucial and essential component of IT governance.

Its importance:

* Maintaining high-quality information to support business decisions.
* Achieving operational dominance through the genuine and organized use of technology - Maintaining IT-related risk at a level where it is manageable - Increasing the worth of IT technology and services
* Comply with key regulations, laws, fair agreements, and plans or policies that are continually expanding in importance.

Effective information security governance requires management's construct and keep up a structure to direct the growth and supervision of a thorough information security program that supports goals for the business.

1. The standard international principles;

* Consistency with all legal systems
* The use of a common language
* Durability
* The ability to cross international boundaries
* The ability to instill confidence in the integrity of evidence
* Applicability to every forensic evidence
* Applicability at every level, which includes that of individual and agency

**QUESTION NUMBER: (e.g., Q2) \_\_2\_\_\_SUB-QUESTION (e.g., 2(a)) \_\_2A, B, C\_**

1. Hjk
2. Elements that need to be considered when performing a project benefits realization:

* Getting ready the benefit that would be gained
* logging the supposition
* Verifying the advantage mentioned in the company
* preparing crucial tasks for completion
* defining and achieving benefits management
* A measure and a mark are assigned.
* establishing a measuring or following administration

1. The models include;

Preparation: In the forensic process, it is the initial stage. This procedure primarily involves questions about the presence of evidence, where it is kept, and how it is kept (in which format). Personal computers, mobile phones, PDAs, and other devices can all include electronic storage media.

Gathering: entails finding, gathering, and preserving evidence using tested methods. The identification, gathering, and preservation of digital evidence are the main actions and tasks in this second stage of the investigative workflow.

Processing: data is revealed and volume is reduced based on contextual and content relevance.

Presentation: includes preparing reporting documentation. The documentation is a crucial component of every investigation that must begin at the outset and continue all the way through the case's resolution. Despite the fact that different types of documentation (such as chain of custody records and specialized notebooks) may be required at different times throughout an investigation, they must always be precise, thorough, and complete.