# PAN AFRICA CHRISTIAN UNIVERSITY

**BACHELORS OF INFORMATION COMMUNICATION TECHNOLOGY**

**END OF TERM EXAMINATION**

**DEPARTMENT:** **COMPUTING & INFORMATION TECHNOLOGY**

**COURSE CODE:** **BSIT/BBIT 402**

**CAMPUS:** **ROYSAMBU**

**COURSE TITLE:** **INFORMATION SYSTEMS AUDIT & CONTROLS**

**EXAM DATE:** **FRIDAY 5:30PM**

**TIME:**

**INSTRUCTIONS**

- This exam carries a total of SIX Questions of [10 Marks Each]
- Section One (I) is compulsory.
- Answer any 3(Three) Questions from Section Two (II)
- Read all questions carefully before attempting.

## Section One Compulsory 10 marks

## Question One.

Investigation Case Study No. 001

*Let's say an investigator responds to the scene of a missing 14-year-old girl. The investigator notices a laptop computer on a desk in the girl's bedroom. Closer scrutiny reveals that the laptop is live and what appears to be an instant message conversation is on the screen.*
*Additionally, what can be seen of the conversation discusses a meeting with what appears to be an older man.*
*The investigator needs to start the process of identifying the individual in the conversation. Almost simultaneously, the investigator needs to preserve the evidence that probably exists only in RAM.*
*Here a consideration of "order of volatility" must be made. The fact that the investigator*
*needs to work with the computer system means that changes to the data (i.e., the electronic crime scene) will be made. Considering order of volatility allows the investigator to develop a sequence of steps that will limit the effects of each change on the subsequent steps and collection methods, thus affording the collection of the greatest amount of unaltered evidentiary data.*
*In this example steps might be completed in the following order:*
*1. Photograph all sections of the conversation screen to document the conversation in the same form the user sees. Merely scrolling through the conversation to afford photographing the entire conversation is minimally intrusive, and limited (and arguably inconsequential) changes will occur.*
*2. Depending on his or her own skill level, the investigator may want to acquire the contents of RAM at this point. This would be accomplished by running a controlled application that the investigator already possesses and that is designed for such a purpose. Of course, the resulting content needs to be written somewhere, and it should not be written to the computer's hard drive.*
*Rather, the examiner should use a clean piece of media that can handle the size of the output. There are several options for this.*
*3. Next, the investigator may want to consider copying the text and pasting it to a new document or using a save command in the chat application to save the conversation in text format. Again, this conversation should not be saved to the hard drive of the system being examined.*
*4. If the investigator feels that encryption is being used, he or she may consider imaging the entire hard drive in this live environment. Because shutting down the computer with encryption in place renders the hard drive's contents unreadable without a password, it may be a good idea to get an image of the hard drive while it is still decrypted. This requires special response tools and external media that can handle the large image size.*
*This is just one way to approach this and other live examinations. The order of steps can also be debated among forensic examiners. The following questions are important for the forensic examiner to consider:*

i. Examine the type of case you'll be investigating and why. **[1 mark]**

ii. Discuss TWO types of evidence available for your case investigations. **[2 marks]**

iii. Describe How best can one acquire this evidence without contaminating other aspects of the electronic crime scene. **[2 marks]**

iv. Define the order should you take your steps and why. **[2 marks]**

v. Describe any THREE types of audit tools one may need to accomplish the evidence collections and processing exercise. **[3 marks]**

**Section Two Attempt any Three Questions.**

**Question Two.**

a) As a lead a team member in writing the final audit report performed at the Kenyan Parliament in vetting of the nominees selected by the President, demonstrate how the three Elements in the fraud Triangle could have compromised the approval process by the sitting members of Parliament**.** **[6 marks]**

b) Banking fraud investigation Department **(BFID)** formerly widely known as the Exchange Control Investigation unit monitors fraud related cases reported from commercial banks and financial institutions. Illustrate FOUR key Functions of BFID. **[4 marks].**

**Question Three**

a) During the semester You did a case study survey reading and analysis on an audit report detailing a disaster recovery plan for a small business called Lipscomb & Pitts Insurance LLC. Based on your own audit recommendations,

   i. Discuss FIVE most common causes of data losses in most small & medium sized companies. **[5 marks].**

   ii. Give recommendations and solutions for the vulnerabilities you've stated in (i) above. **[5 marks]**

**Question Four**

a) Discuss TWO common Cloud or network attached storage privacy issues. **[2 marks].**

b) While Auditing Operating systems in distributed systems architecture environment and Hardware appliances supplied to Banking Institutions, You watched a tutorial video clip on how crooks would use the V-Mark code to make standalone ATM spill out money.

i. Analyze **TWO** main approaches or weaknesses on how the above felony could be executed. **[4 marks]**

ii. Propose **TWO** applicable solutions to mitigate the weaknesses you specified. **[4 marks]**

**Question Five.**

**a)**

Your ABC Audit firm has been awarded a tender to participate in auditing Kenya's Independent Electoral & Boundaries Commission (IEBC) after the last concluded election. Discuss FOUR Key objectives that ABC firm would seek to accomplish. **[4 marks].**

**b)** Analyze the following THREE *provisions of ECPA.*

i. Title I (Wiretap Act). [**2 marks]**

ii. Title II Stored Communications Act (SCA). [**2 marks]**

iii. Title III (The Pen/Trap Statute). [**2 marks]**

**Question Six.**

a) All audits follow a similar sequence of activities and may be divided into four stages: (Planning, collecting evidence, evaluating evidence and Communicating audit results Discuss the metrics you would apply as an Auditor at all the above stage/level. **[8 marks]**

b) Differentiate between Actus Reus & Men's Rea. **[2 marks]**

**-END-**