PAN AFRICA CHRISTIAN UNIVERSITY

BACHELOR OF SCIENCE INFORMATION TECHNOLOGY AND BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

END OF SEMESTER EXAMINATION

DEPARTMENT:	**COMPUTING AND INFORMATION TECHNOLOGY**
COURSE CODE:	**BSIT402/ BIT402**
COURSE TITLE:	**INFORMATION SYSTEMS SECURITY AND AUDIT**
CAMPUS:	**ROYSAMBU**
EXAM DATE:	**TUESDAY,XXXX,APRIL,2026**
TIME:	**2:00PM -4:00PM**

INSTRUCTIONS

- This exam script has **TWO (2)** sections.
- Read all questions carefully before attempting.
- Answer All questions in Section **A** and any other Three questions in Section **B.**
- Write only your **student number** on the answer booklet provided.

SECTION A
(Answer ALL questions in this section)

Question One (15 marks) Compulsory

a) Differentiate between the following terms as used in information systems security;

i. Threat and Vulnerability **[2 Marks]**

ii. Incremental Backup and Differential Backup **[2 Marks]**

b) Describe the three principles of CIA with respect to information systems security.

 © Copyright 2026 All Rights Reserved PAC University

[3 Marks]

c) "A quality information security program begins and ends with policy." Using Bulls' Eye Model, justify this statement. **[3 Marks]**

d) Computers have become integral part of everyday life and a s such, precautions should be taken to protect them from viruses, spyware, ransomware and persistent threats from hackers. Knowing that there is no single method that guarantees such protection, Discuss three protection measures for our electronics gadgets like computers and mobile devices. **[3 Marks]**

e) Explain two types of Intellectual Property Rights. **[2 Marks]**

SECTION B
(Answer any THREE (3) questions in this section)

Question Two (15 Marks)

a) Explain the following types of social engineering attacks.

i. Vishing
ii. Phishing
iii. Biting **[6 Marks]**

b) Outline any three environmental threats/hazards to information systems resources. **[3 Marks]**

c) With the advancements in mobile technology and network infrastructures, companies all around the world now allow their workforce to work from their point of convenience like homes, coffee shops, restaurants, hotels etc. With such flexibilities and ability to connect to company intranet from multiples locations and

 © Copyright 2026 All Rights Reserved PAC University

devices, maintaining high level security has become more critical than ever. Discuss three guidelines to allow employees work remotely and securely. **[6 Marks]**

Question Three (15 Marks)

a) The codes of professional ethics states that an auditor shall "perform their duties with objective, due diligence, and professional care, in accordance with professional standards and best practices". Explain what is meant by: **[9 Marks]**

i. Objectivity
ii. Due diligence
iii. Professional care

b) Information system auditing makes reference to the following documents:

i. Policies
ii. Standards
iii. Guidelines

Describe each and how the three documents are related. **[6 Marks]**

Question Four (15 Marks)

a) Any information system or data processing system, whether computerized or not, must incorporate controls to ensure that it works efficiently. Discuss three computer system controls. **[6 Marks]**

b) An insurance company X has in the recent past experienced tremendous growth and consequently grown and expanded in branch network. In one of the local branches, its performance has been out of line with the rest of the branches. The management has decided to send auditors to unearth the reasons for its dismal performance. In their course of duty, they discover serious security breaches with

 © Copyright 2026 All Rights Reserved PAC University

how data computer is kept and backed up. Additionally, there is indiscriminate use of computer resources including internet access by all and sundry. As an Information security Expert;

i. Explain the term computer control. **[2 Marks]**

ii. Outline two unethical behaviors in the company. **[2 Marks]**

iii. State the difference between internal and external audit. **[2 Marks]**

iv. Highlight three reasons why the organization decided to conduct the audit other than dismal performance.
[3 Marks]

Question Five (15 Marks)

a) Differentiate between Software Security and Cyber Security. **[2 Marks]**

b) Denial-of-service attacks come in a variety of forms and target a variety of services. State four major problems that these attacks may cause. **[4 Marks]**

c) Outline three factors to be considered when developing any security controls to ensure that they are cost-effective. **[3 Marks]**

d) Explain the following types of malware threat; **[6 Marks]**

i. Computer virus
ii. Worm
iii. Trojan Horse

Question Six (15 Marks)

a) State three benefits of implementing COBIT as a governance framework. **[3 Marks]**

 © Copyright 2026 All Rights Reserved PAC University

b) Suppose that you have been appointed as chief security officer with an organization.

You have been given the task of carrying out an audit on the information security systems of the organization. Describe four steps you will involve in carrying out the task. **[4 Marks]**

c) Discuss the roles of the following Information Technology resources as defined in COBIT framework.

i. Organizational Structures **[2 Marks]**

ii. Application systems **[2 Marks]**

iii. Information **[2 Marks]**

iv. People **[2 Marks]**

END

 © Copyright 2026 All Rights Reserved PAC University