NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR HONOURS OF COMPUTER SCIENCE	
QUALIFICATION CODE: 07BACS	**LEVEL: 8**
COURSE: CRITICAL INFRASTRUCTURE PROTECTION	**COURSE CODE:** CIP821S
DATE: NOVEMBER 2019	**SESSION: 1**
DURATION: 3 HOURS	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. MBAUNGURAIJE TJIKUZU**
MODERATOR:	**MR ATUMBE BARUANI**

INSTRUCTIONS

1. Answer **all questions**.
2. Please, ensure that your writing is **legible, neat** and **presentable.**
3. When answering questions you should be led by the allocation of marks.
4. Clearly mark rough work as such or cross it out unambiguously in ink.

PERMISSIBLE MATERIALS

1. Calculator

THIS QUESTION PAPER CONSISTS OF 4 PAGES (Including this front page)

Question 1 **[20 Marks] [2 Marks/ correct answer]**

I. What is the main purpose of cyberwarfare?

a) to protect cloud-based data centers

b) to gain advantage over adversaries

c) to develop advanced network devices

d) to simulate possible war scenarios among nations

II. What is an essential function of SIEM?

a) providing reporting and analysis of security events
b) providing 24×7 statistics on packets flowing through a Cisco router or multilayer switch
c) monitoring traffic and comparing it against the configured rules
d) forwarding traffic and physical layer errors to an analysis device

III. Which two options are security best practices that help mitigate BYOD risks? (Choose two.)

a) Use wireless MAC address filtering.
b) Decrease the wireless antenna gain level.
c) Keep the device OS and software updated.
d) Only turn on Wi-Fi when using the wireless network.
e) Only allow devices that have been approved by the corporate IT team.
f) Use paint that reflects wireless signals and glass that prevents the signals from going outside the building.

IV. What are three access control security services? (Choose three.)

a) availability
b) authentication
c) authorization
d) repudiation
e) accounting
f) access

V. Which three are major categories of elements in a security operations center? (Choose three.)

a) people
b) processes
c) data center
d) technologies
e) database engine
f) Internet connection

Question 2 [25 Marks]

Scenario 1: Unauthorized Access to Payroll Records

Study the following scenario. Discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a mid-sized hospital with multiple satellite offices and medical services. The organization has dozens of locations employing more than 5000 employees. Because of the size of the organization, they have adopted a CSIRC model with distributed incident response teams. They also have a coordinating team that watches over the CSIRTs and helps them to communicate with each other.

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The security teams practice the kill chain model and they understand how to use the VERIS database. For an extra layer of protection, they have partially outsourced staffing to an MSSP for 24/7 monitoring.

Question 3 **[15 Marks] [5 Marks/ Question]**

a) As Return of Investment (ROI) can be used to calculate the effectiveness of risk reduction, calculate the ROI of the following scenario:

- Risks before control measures = N$100,000 (Hundred Thousand)
- Risks after control measures = N$10,000 (Ten Thousand)
- Total investment made = N$45000 (Forty-Five Thousand)

b) Using Probability Risk Analysis, calculate the estimated risk value when the following condition prevails:

- Estimated threat probability = 0.1
- Estimated damage probability = 0.25
- Estimated losses = N$100000.00

c) What is the risk of successful cyber-attacks in Namibia and Total Power Blackout? Given the following variables and conditions:

P(Cyber-Attacks) = 14%; C (Cyber-Loss) = N$100 Million
P(Blackout) = 20%; C (Blackout) = N$0.5Million
Calculate the risk estimate for both together.

Question 4 **[40 Marks]**

a) How can government institution leverage ISAC capabilities to enforce and mature cybersecurity? [10]

b) Explain the definition, applicability, and differences of "Trustworthiness, Functionality and Assurance" for critical infrastructure protection. [30]

>>>END OF QUESTION PAPER>>>