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: JANUARY 2020	SESSION: 2
DURATION: 3 HOURS	MARKS: 100

SUPPLEMENTARY/SECOND 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 3 PAGES (Including this front page)

Question 1 [44 Marks]

a) Why is it important to protect all accounts with strong passwords? [2]
b) Why would you create a user with Standard privileges? [2]
c) What are your major considerations in implementing cybersecurity and privacy controls? [10]
d) What do you understand by a "control baseline"? What factors must you consider in creating an appropriate "Control Baseline"? [10]
e) How does the adoption of a Risk Management Framework help critical infrastructure in terms of cybersecurity? [10]
f) What are the possible functions that an Information Sharing and Analysis Center?

Question 2 [25 Marks]

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Study the following scenario and 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 small, family-owned investment firm. The organization has only one location and less than 100 employees. On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. It was several hours after the worm started to spread before antivirus signatures became available. The organization had already incurred widespread infections.

The investment firm has hired your team of security experts who often use the diamond model of security incident handling.

Question 3 [16 Marks]

a) What are the three methods used in social engineering to gain access to information? [6]
b) What are three examples of social engineering attacks from the first two methods in step a)? [6]
c) Why is social networking a social engineering threat? [2]
d) How can an organization defend itself from social engineering attacks? [2]

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$300,000 (Hundred Thousand)
   - Risks after control measures = N$50,000 (Ten Thousand)
   - Total investment made = N$100000 (Forty-Five Thousand)

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

- Estimated threat probability = 0.2
- Estimated damage probability = 0.4
- Estimated losses = N$50000.00

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

- P(Cyber-Attacks) = 10%; C (Cyber-Loss) = N$50 Million
- P(Blackout) = 30%; C (Blackout) = N$20 Million
- Calculate the risk estimate for both together.