# FACULTY OF SCIENCE

| ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING | |
|---|---|
| MODULE | IT00280/IT28X80/IT00299/IT8X299<br>INFORMATION SECURITY GOVERNANCE |
| CAMPUS | APK |
| EXAM | JANUARY 2019 SUPPLEMENTARY |

DATE: 29 January 2019 SESSION: 15:00 – 10:00

ASSESSOR (S) Prof SH von Solms
Dr. MR Corregedor

INTERNAL MODERATOR

EXTERNAL MODERATOR Dr. J van der Merwe (DVT)

DURATION: 2 Hours MARKS: 100

THIS PAPER CONSISTS OF 3 PAGES INCLUDING THE COVER PAGE

INSTRUCTIONS:

1. Answer ALL the questions
2. Read the questions thoroughly
3. Write neatly and legibly
4. Answer Part 1 and Part 2 in two different answer books
5. Ensure that all questions are clearly marked on the answer sheet.
6. Ensure that all questions are answered in a logical and structured form which is easy to read and follow. Marks will specifically be assigned for these aspects.

REQUIREMENTS: NONE

Part 1 (Consists of 1 question only)

Question

You have received an invitation from the Editor of the highly acclaimed Journal of Corporate Governance (JCG) to write an article for the Journal.
The Editor also informs you that the Journal is dedicated to Board Members of companies, Executive Management and other senior stakeholders, and is widely read by this specific community.
The Editor asks you to write a general article explaining, in a simple and readable way, the aspects related to Information Security Governance. The purpose of your article is to provide a well structured and readable discussion to convey the concept of ISG to the reader community of the JCG.

Amongst other aspects, you must clearly explain the following:

a) What is Information Security Governance (ISG)? The goal of your answer must be to highlight the fact that ISG is much more than just technology.
b) Where does ISG fit into the wider architecture of Governance in general? Refer to and discuss national and international documents to motivate your explanation.
c) Why is ISG important to the reader community (Board members and Executive Management) of the JCG? Refer to case studies to make your point.
d) What is the responsibility of the reader community (Board members and Executive Management) of the JCG towards ISG in their companies?
e) What are the personal consequences to Board Members and Executive management which can result from ignoring ISG in their companies? Refer to case studies to support your explanation.
f) How can the reader community (Board members and Executive Management) of the JCG ensure that the ISG in their companies is on an acceptable level?

Write the article along the lines suggested by the Editor. Clearly structure the article according to the 6 aspects mentioned by the Editor.

Marks will be assigned as follows:
8 marks for presentation, structure, logic, readability and general 'feeling' of the article.
42 marks for the content covered for the 6 aspects mentioned above, and others if included.
Student must spend, on average, the same amount of time and effort on the 6 aspects above.

[50]

Part 2 (Consists of 1 question only)

Question

Your organisation which has a large national footprint has unfortunately suffered a cyber security breach where personal information of clients was stolen and leaked online. This has resulted in a negative impact on the organisation's reputation which has negatively affected revenue. The board is rightfully concerned and has asked you, in your capacity as CSO (Chief Security Officer), to provide them with a Plan to ensure that this never happens again. At a high level, the board requires that the following be considered:

a) Cyber Security Governance
   - The board signed an information security policy a few years ago. Is this not sufficient in terms of covering cyber security?
   - We currently on the road to ISO 27001 certification, is this sufficient? Do we require looking at additional standards and / or frameworks?
   - How can we improve our Governance, Risk and Compliance to better address Cyber Security threats?

b) Training and Awareness

   A large amount of our budget has been allocated towards awareness and training, however, given our recent incident the board feels the budget for training and awareness should be allocated to technology controls instead. What are your recommendations regarding this?

   Justify your response above by providing examples and, if applicable, plans that would be required.

c) Incident Response

   The board learnt of the breach from the media. How can this be improved upon in the future?

   What can we do to better improve our response and recovery controls?

   Can you guarantee that this will never happen again?

Write this Plan required by the board, covering the aspects mentioned in a), b) and c).

Marks will be assigned as follows:
8 marks for presentation, structure, logic, readability and general 'feeling' of the article.
42 marks for the content covered for the a), b) and c) mentioned above, and others if included. Students must spend, on average, the same amount of time and effort on a), b) and c).

[50]

TOTAL: [100]