FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING	
MODULE	IT00280/IT28X80/IT00299/IT8X299 INFORMATION SECURITY GOVERNANCE
CAMPUS	APK
EXAM	JANUARY 2017 – SUPPLEMENTARY

DATE: January 2017 SESSION: 8:30 – 10:30

ASSESSOR (S) Prof SH von Solms

INTERNAL MODERATOR

EXTERNAL MODERATOR Dr J van der Merwe (DVT)

DURATION: 2 Hours MARKS: 100

THIS PAPER CONSISTS OF 5 PAGES INCLUDING THE COVER PAGE

INSTRUCTIONS:

1. Answer ALL the questions
2. Read the questions thoroughly
3. Write neatly and legibly
4. Ensure that all questions are clearly marked on the answer sheet.

REQUIREMENTS: NONE

Question 1

You are the newly appointed Chief Information Officer (CIO) of your company, and you receive the following memo from the Chief Executive Officer (CEO) of your company:

'Last week I attended a seminar on Information and Cyber Security Governance (ICSG). One of the speakers referred to two documents she called ISO 27002 and ISO 27001.

She strongly urged companies to take note of these Best Practice documents when creating and maintaining their Information Security Governance plans. She specifically emphasized ISO 27002 as a good document to use for a 'health check' and ISO 27001 as a preferred route to follow for the 'formalization' of the company's Information Security approach.

Please provide me with a 5 page document on the following aspects:

1. *Item 1 : Explain*

    1.1 what ISO 27002 is
    1.2 what ISO 27001 is

In both 1.1 and 1.2 above, cover aspects like

- *the history of the document*
- *the purpose of the document*
- *the structure of the document*
- *the way in which we can use the document in our company*

1.3 the relationship between the two documents

2. *Item 2: Provide a comprehensive Implementation Plan (IP) on how our company can use these two documents to get our Information Security Governance level up to an acceptable standard. Address the aspects of a 'health check' and 'formalization' as referred to by the speaker.*
   The IP must be logical, provide a clear step by step implementation approach, must indicate how the two documents discussed above must be used and what benefits we can get from following that route.

As I intend to submit your report to the Board, please ensure that the document is logical, well structured, easy to follow and covers all the aspects I mentioned above.'

Write this document requested by the CEO specifically referring to the aspects mentioned above.

Marks will be assigned as follows for the different aspects mentioned in the CEO's memo:
Item 1: 20
Item 2: 20
Presentation as far as logic, clarity, comprehensiveness and readability: 10

Important: Structure your answer as close as possible to the theory and discussion covered during the lectures.

[50]

Question 2

Immediately after the CEO's memo in Question 1, you get a second memo from the CEO.

'*At the same seminar I attended last week, another speaker emphasized the importance of compliance enforcement methods, methodologies and tools to ensure that Information Security policies are being complied with and that Information Security risks can be reported to the Board. She called this the 'Control' part of the 'Information Security Governance loop'.*

Please provide me with a 2 page document on the following aspect:

1. *An explanation of what this 'Information Security Governance loop' is, and where the 'Control' part fits in.*
   Also describe what mechanisms and tools we can use to enforce this 'Control' part of the loop.

   As I intend to submit your report to the Board, please ensure that the document is logical, well structured, easy to follow and covers all the aspects I mentioned above.'

Write this document requested by the CEO.

Marks will be assigned as follows for the different aspects mentioned in the CEO's memo:
Item 1: 18
Presentation as far as logic, clarity, comprehensiveness and readability: 7

Important: Structure your answer as close as possible to the theory and discussion covered during the lectures.

[25]

Question 3

Immediately after the CEO's memo in Question 2, you get a third memo from the CEO.

'*In their latest Audit Report, the external auditors were very critical about the status of specifically Cyber Security in the company. They claimed that the Board of the company is not aware of the Cyber Security accountabilities and responsibilities and that they very much see Cyber Security as something that has nothing to do with them.*

Please provide me with a 2 page document on the following aspect:

1. *Explain*

    1.1 Why the Board has such Cyber Security accountabilities and responsibilities
    1.2 What the consequences can be if the Board ignores these accountabilities and responsibilities
    1.3 How we can go about to make the Board aware and keep them aware of Cyber risks to the company.

In your explanation, refer to international documents which can support your view. As I intend to submit your report to the Board, please ensure that the document is logical, well structured, easy to follow and covers all the aspects I mentioned above.'

Write this document requested by the CEO.

Marks will be assigned as follows for the different aspects mentioned in the CEO's memo:

Item 1: 20
Presentation as far as logic, clarity, comprehensiveness and readability: 5

Important: Structure your answer as close as possible to the theory and discussion covered during the lectures.

[25]

TOTAL [100]