DEPARTMENT OF APPLIED INFORMATION SYSTEMS

COLLEGE OF BUSINESS AND ECONOMICS

SCHOOL OF CONSUMER INTELLIGENCE AND INFORMATION SYSTEMS

EXAMINATION

MODULE	: PROTECTION OF INFORMATION ASSETS
CODE	: PGD004
DATE	: 23 NOVEMBER 2017
DURATION	: 2 HOURS
TIME	: 12H30
TOTAL MARKS	: 100

LECTURER	: MRS MAUREEN VAN DEN BERGH
MODERATOR	: PROF TRANOS ZUVA
NUMBER OF PAGES	: 4 PAGES

INSTRUCTIONS TO CANDIDATES:

- Please answer all questions.
- This question paper remains the property of the university and must be handed over to the invigilator before leaving the examination venue.
- This is a closed book assessment.
- Read the questions carefully and answer only what is asked.
- Number your answers clearly.
- Write neatly and legibly.
- Structure your answers by using appropriate headings and sub-headings.
- The general University of Johannesburg policies, procedures and rules pertaining to written assessments apply to this assessment.

CASE STUDY

Électricité de France (EDF)

Électricité de France (EDF) is Europe's largest electricity utility company, and is the second largest in the world. Headquartered in Paris and listed on France's CAC exchange, the group posted €65.3bn in revenues in 2011. It has two principal business arms in the UK – EDF Energy and EDF Trading – and operates a diverse portfolio of 120,000+ megawatts of generation capacity in Europe, Latin America, Asia, the Middle East and Africa.

EDF's UK audit director, Alistair Smith, has implemented a risk-based internal audit approach as he believes that this is the best way to add value and provide assurance to the two audit committees in the UK (one for each business), the corporate audit team based in Paris and the group board.

"Internal audit's role is to provide assurance that key risks to the organisation's objectives are being well controlled. As a result, it makes sense that our audit programme is prioritised based on risk," he says.

Prioritising risk

Both EDF Energy and EDF Trading have separate risk management functions that are responsible for establishing risk policy, for supporting line managers in the development of a risk register and for co-ordinating the reporting of risks to the executive. As part of its reviews, internal audit monitors the effectiveness of risk management arrangements.

EDF Energy's corporate risk policy sets out a three-tier approach to how people assess and report risks. These are listed as "critical", "significant", or "registered". While critical risks are prioritised by the business, Smith and his team of 20 internal auditors review them to see if the business' assessment is consistent with its findings. The EDF Trading risk policy and classification is separate, but the same audit approach applies.

As part of the planning process, the internal audit team looks at the organisation's risk register to see if it is complete and that there are no major risks missing. The function also considers which of these risks would have the most serious impact if controls were ineffective.

"The business scores these risks on the basis of controls that are in place rather than on an inherent basis, which means that there is a danger that some may be understated. When developing our audit plan, we need to consider whether the controls in place are well-designed and are working," says Smith. "Equally, we can add value by pointing out where too much resource is being targeted at risk control."

"One of the key steps to success with a risk-based approach is for internal audit to talk to the board and senior management to ensure that their 'top-down' view of big risks aligns with what internal audit has found in 'bottom-up' risk registers and from its current reviews" – Alistair Smith, EDF

CASE STUDY QUESTIONS

Q1. Before the actual audit is performed, Alistair Smith's team will first plan and prepare this process. What steps will they follow to plan for the audit process? **[7 Marks]**

Q2. When the auditing team create the document to be signed by new IT users, employees or 3rd parties, they should ensure that the document contain the main IT security obligations that these individuals should know and observe. Discuss the security obligations that should be included in this document. **[8 Marks]**

Q3. When protecting assets, physical access controls are just as important as logical access controls. Which type of physical access controls should Alistair's team take into consideration when protecting Électricité de France's assets? **[15 Marks]**

GENERAL QUESTIONS

Q4. During the process of Information Security Management, what would be the role of the Information Systems (IS) steering committee? **[3 Marks]**

Q5. Discuss the eight elements that should be included in the inventory record for any asset. **[8 Marks]**

Q6. What is authorization creep and how should it be managed? **[4 Marks]**

Q7. In the context of human resources security, what should be clearly stated within the terms and conditions of an employment document? **[7 Marks]**

Q8. What is the difference between?

(a) Phishing **(3)**

(b) spear phishing **(3)**

(c) and pharming **(4)**

[10 Marks]

Q9. In the context of cryptography:

(a) What does the $P = D(K, E(K, P))$ algorithm represents? **(2)**

(b) Identify each of the elements in the algorithm and explain the meaning of this algorithm. **(8)**

[10 Marks]

Q10. When using physically oriented biometrics, an organisation may use several options:

(a) List six types of physically oriented biometrics and give a short description of each one. **(12)**

(b) For each of the physically oriented types of biometrics, discuss one advantage and one disadvantage. **(12)**

[24 Marks]

Q11. Explain what an Intrusion Detection System (IDS) is. **[4 Marks]**

----------[TOTAL 100 MARKS]----------