NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Informatics

QUALIFICATION : BACHELOR OF INFORMATICS HONOURS (BUSINESS INFORMATICS)	
QUALIFICATION CODE: 08BIH	**LEVEL:** 8
COURSE CODE: ISA822S	**COURSE:** INFORMATION SYSTEMS AUDIT
DATE: NOVEMBER 2019	**PAPER:** THEORY
DURATION: 3 Hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR MUNYARADZI MARAVANYIKA
MODERATOR:	MR PANDULENI NDILULA

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. Do not use additional materials
5. Cross out any work which should not be marked.
6. No pencil work allowed except for diagrams where requested.

THIS QUESTION PAPER CONSISTS OF 3 PAGES
(Excluding this front page)

Use the scenario below to answer SECTION A. The answers should be relative to the context.

Case Study: WorldCom

Prior to filing bankruptcy in 2002, WorldCom was the second largest telecommunications company in the world. It handled Internet data traffic globally and accounted for more international voice traffic than any other company. WorldCom grew quickly from its modest beginning in 1983 and achieved its tremendous growth through 65 acquisitions. In the 1990s, the company made some large acquisitions, including MCI Communications. Through this period, WorldCom spent approximately $60 billion and accumulated approximately $41 billion in debt. The MCI acquisition was the largest merger in U.S. history at the time.

The market value of WorldCom continued to grow substantially through these acquisitions, and high expectations continued to be placed on the company. This generated pressure to keep the stock price at elevated levels, which in turn allowed WorldCom to continue its acquisition spree. A proposed merger in 2000 with Sprint would have eclipsed the merger with MCI; however, the merger was disapproved, and WorldCom started to unravel. In an attempt to maintain its earnings, WorldCom liberally interpreted accounting rules to make its financial statements seem profitable. The company soon moved from liberal interpretation into outright fraud by creating false entries.

A team of internal auditors became suspicious over numerous financial oddities and began investigating, but the auditors encountered problems. They tried to discuss financial irregularities with WorldCom's external auditors, Arthur Andersen, who did not fully cooperate. Responsible to the WorldCom chief financial officer (CFO) at the time, the internal audit group raised issues with the CFO but was pressured to stop. The internal auditors persisted and eventually uncovered what would become the largest account fraud in U.S. history.

How could this have happened, and what were some of the events and situations that led to this mess?

- The board of directors became simply a "rubber stamp."
- The board of directors allowed the chief executive officer (CEO) and CFO of WorldCom to have unfettered power.
- WorldCom acquired many companies without a strategy for linking them properly.
- The board of directors approved deals worth billions of dollars with little discussion.
- Little oversight of debt accumulation existed.
- Little oversight of company loans made to the CEO existed.
- The company lacked internal controls and transparency.

- External consultants failed to apply techniques consistent with their risk rating of the company.
- Internal auditing was underqualified and focused on non-auditing activities.

SECTION A: CASE STUDY **[30 MARKS]**

1. How do a company's acquisitions relate to risk management and governance? [5]
2. The WorldCom scandal resulted in steps to improve standards, controls, and accountabilities. How much do morals contribute to such events and what can be done to address this issue? [5]
3. How might a control framework for IT that is more closely aligned with business processes have prevented this? [5]
4. How could adequate controls on IT systems and financial applications have helped?[5]
5. Briefly discuss whether controls designed to prevent or detect fraud were in place and their adequacy? [5]
6. Discuss the importance of continuous monitoring of such controls, and how should access be controlled? [5]

SECTION B: STRUCTURED QUESTIONS **[70 MARKS]**

1. Software Acquisition **[20 Marks]**

Over the years, business application development has occurred largely through the use of the traditional SDLC phases, also referred to as the waterfall technique. Briefly describe the six phases of the traditional SDLC and outline the auditor's role in each of those phases.

2. Information systems/information technology governance **[20 Marks]**

As the IT business continuity strategy and its overarching IT strategy are executed, the IT infrastructure of the organization changes. New risk countermeasures are introduced and old ones become obsolete. The information system BCP must be changed accordingly and retested periodically to ensure that these changes are satisfactory. Business Impact Analysis (BIA) is a critical step in developing the business continuity strategy and the subsequent implementation of the risk countermeasures and BCP in particular. Using an appropriate example, discuss the three important BIA considerations.

3. Audit and development of application controls **[10 Marks]**

a. In today's environment, the threat of computer viruses is high because of the unlimited number of sources from which they can be introduced. Computer viruses can be copied from a disk, downloaded from an infected Web page, spread among computers connected within a network, etc. Describe the risks or problems that may result from computer viruses in the context of the NTI case. [5]

b. Application controls can be described as techniques used to control the input, processing, and output of information in an application. Distinguish between input controls, output

controls and program controls. [5]

4. **Information Security Management** **[20 Marks]**

Laying the foundation for effective information security management is the most critical factor in protecting information assets and privacy. Discuss the key elements of Information Security Management.

END OF PAPER!