

**MAKERERE UNIVERSITY BUSINESS SCHOOL**  
**COURSEWORK TWO TEST FOR THE DEGREE OF BACHELOR OF SCIENCE IN**  
**ACCOUNTING OF MAKERERE UNIVERSITY AY 2025/2026**

**COURSE NAME:** Risk Management & Forensics in Accounting

**YEAR OF STUDY:** Three

**COURSE CODE:** BSA3211

**DATE:** APRIL 19, 2026

**SEMESTER:** Two

**TIME:** 5:30PM - 6:30PM

---

***Instructions:***

❖ *Answer ALL questions.*

❖ *The test is based on a practical banking scenario. Show clear understanding and application.*

---

**Question 1**

Kawempe Commercial Bank Ltd is a mid-sized financial institution operating in Uganda with several branches across the country. Recently, the bank experienced a major system disruption following a cyber-attack that affected its online banking platform and temporarily halted customer transactions.

During the disruption, customers were unable to access their accounts, and internal operations were significantly affected. The bank's management activated its Business Continuity Plan (BCP), allowing some critical services such as over-the-counter withdrawals and internal fund transfers to continue manually.

Following this incident, the Board of Directors requested both the Internal Audit Department and the External Auditors to assess the situation.

**Required**

- a)** Differentiate between Business Continuity Management (BCM) and Business Continuity Planning (BCP). [6 Marks]
- b)** Discuss any four key objectives of BCM and explain how each objective is relevant to Kawempe Commercial Bank Ltd in the event of the cyber-attack. [8 marks]
- c)** Prepare concise talking points for presentation at the MUBS Internal Audit Symposium, clearly distinguishing the roles of Internal Audit and External Audit in risk management in terms of focus, scope, timing, reporting, and overall objectives. [16 marks]

*Note: Support ALL your answers with practical examples from the case.*

***End of the test paper***

**MAKERERE UNIVERSITY BUSINESS SCHOOL  
BACHELOR OF SCIENCE IN ACCOUNTING  
RISK MANAGEMENT & FORENSICS IN ACCOUNTING  
MARKING GUIDE FOR TEST TWO**

**(a) Difference Between Business Continuity Management (BCM) and Business Continuity Planning (BCP)**

Aspect	Business Continuity Management (BCM) <i>[Any 2 correct points x 1 mark = 2 marks]</i>	Business Continuity Planning (BCP) <i>[Any 2 correct points x 1 mark = 2 marks]</i>	Application to Kawempe Commercial Bank Ltd Case <i>[Any 2 correct points x 1 mark = 2 marks]</i>
Scope	A broad, organization-wide framework that manages business continuity as a whole	A specific component that contains documented procedures for responding to disruptions	The bank's BCM framework guided how it should respond to the cyber-attack, while the BCP provided step-by-step actions such as switching to manual withdrawals
Nature	Continuous, proactive, and strategic management process	A documented, operational response plan used during incidents	BCM ensured the bank was prepared for cyber risks, while BCP was activated during the system failure
Purpose	Builds resilience and ensures long-term operational stability	Ensures immediate response and short-term recovery of operations	BCM aimed to ensure the bank could withstand future cyber-attacks; BCP enabled continued service during the outage
Ownership	Driven by senior management, risk management, and the Board	Implemented by operational units and branch-level teams	Senior management activated BCM oversight, while branch staff implemented manual transaction procedures under the BCP
Focus	Focuses on preparedness, risk reduction, and organizational resilience	Focuses on recovery actions and continuity of critical services	BCM focused on overall cyber resilience; BCP ensured customers could still withdraw money over the counter during the disruption

**2 well-developed differences × 3 marks each = 6 marks**

**(b) Key Objectives of BCM**

- ❖ **Ensuring Personnel Safety.** BCM aims to protect employees and customers during disruptions.  
*Example:* The bank ensured safe manual operations at branches during the system outage, protecting both staff and customers from panic or unsafe situations.
- ❖ **Maintaining Critical Functions.** BCM ensures that essential services continue even during a crisis.  
*Example:* Kawempe Bank continued core services like cash withdrawals and internal transfers manually despite the failure of digital systems.
- ❖ **Rapid Recovery (RTO).** BCM focuses on restoring operations within an acceptable timeframe.  
*Example:* The bank worked to restore its online banking system within a defined Recovery Time Objective to resume normal digital operations.
- ❖ **Minimizing Financial Loss.** BCM reduces losses caused by business interruptions.  
*Example:* By maintaining partial operations, the bank avoided complete shutdown and loss of revenue from transactions.
- ❖ **Protecting Reputation.** BCM helps maintain customer trust and confidence.  
*Example:* Continued service delivery reassured customers and reduced reputational damage during the cyber-attack.
- ❖ **Ensuring Compliance.** BCM ensures adherence to legal and regulatory requirements.  
*Example:* The bank's response would need to comply with Bank of Uganda regulations on operational resilience and reporting incidents.
- ❖ **Building Resilience.** BCM strengthens the organization's ability to handle future risks.  
*Example:* The cyber-attack provides lessons for improving IT security and continuity planning in the future.

**4 well-developed objectives × 2 marks each = 8 marks**

## C) Talking Points for the Head of Internal Audit – MUBS Internal Audit Symposium

### 1.0 Introduction (Context from Case) [0.5 marks]

- ❖ Kawempe Commercial Bank experienced a cyber-attack that disrupted operations and exposed weaknesses in risk management and controls.
- ❖ Both Internal Audit and External Audit played important but distinct roles in responding to these risks.

### 2.0 Key Differences Between Internal Audit and External Audit in Risk Management

Aspect	Internal Audit <i>[Any 5 correct points x 1 mark =5 marks]</i>	External Audit <i>[Any 5 correct points x 1 mark =5 marks]</i>	Application to Kawempe Bank Case <i>[Any 5 correct points x 1 mark =5 marks]</i>
<b>Focus</b>	Focuses on a broad range of risks including operational, IT, financial, and strategic risks.	Narrow focus on financial reporting risks	Internal audit should review the cybersecurity and BCM failures; external audit should focus on accuracy of financial records after the disruption
<b>Scope</b>	Comprehensive – covers all internal controls across the organization	Limited – focuses on controls related to financial statements	Internal audit should examine IT systems, manual processes, and controls; external audit should review only financial reporting controls
<b>Timing</b>	Continuous and proactive throughout the year	Periodic, mainly annual (year-end)	Internal audit could assess risks during and immediately after the cyber-attack; external audit must assess the impact during year-end audit
<b>Reporting</b>	Reports to Board and Audit Committee	Reports to shareholders and regulators	Internal audit should report the weaknesses in controls and BCM to the Board; external auditors will issue an opinion on financial statements
<b>Overall Objective</b>	Improve risk management, internal controls, and operations	Provide independent assurance on financial statements	Internal audit should recommend improvements in cybersecurity and continuity plans; external audit should ensure financial statements reflect the disruption accurately

**5 well-developed differences × 3 marks each = 15 marks**

### 3.0 Conclusion (for Presentation) [0.5 marks]

- Internal Audit is **proactive and improvement-oriented**, focusing on strengthening systems and preventing future risks.
- External Audit is **independent and assurance-oriented**, focusing on the credibility of financial reporting.
- Both functions are complementary and critical in strengthening risk management in banking institutions.