110

University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

UNIVERSITY MAINEXAMINATIONS 2022/2023 ACADEMIC YEAR

THIRD YEAR FIRST SEMESTER EXAMINATIONS FOR THE DEGREE OF BACHELORS OF COMMERCE

COURSE CODE: BCB 361

COURSE TITLE: RISK MANAGEMENT IN SUPPLY CHAIN

DATE: MONDAY, 19TH/12/2022 **TIME:** 3:00 - 5:00PM

INSTRUCTIONS TO CANDIDATES

Question ONE (1) is compulsory
Answer other TWO questions
Do not write anything on the question paper

RAPIDLY GROWING CONSUMER RETAILER

Risk manager Sara is part of the Governance, Risk, and Compliance (GRC) team for a national retailer. With ransomware on the rise, Sara knew it was time to re-evaluate her company's insurance coverage to address the possibility of cyberattack. She contacted her company's insurance provider and received a list of dozens of questions related to security controls and strategies. She went to her Chief Information Securtiy Officer (CISO)—whom she had never met to fill in the answers.

According to David Shluger, Cyber Risk Engineering Lead at Zurich North America, it's common that GRC pros, often the people responsible for procuring insurance, don't have the technical detail at hand. For that reason, his team often helps bridge the gap between GRC and the IT teams responsible for security strategies. As he explains, "we identify a control gap and provide actionable advice to close it."

Unlike regulatory compliance, there is no "one-size-fits-all" security framework required by insurance companies. That's why David's team at Zurich doesn't use a checklist-based approach to evaluating risk. "Each customer has a different threat landscape and may not need identical protection," David notes. "You may have alternative or compensating controls to solve the same issue.

If David and his team identify significant control gaps, they will collaborate with the Underwriter to determine the level of residual risk, and whether it is a good fit. "Our appetite for risk isn't a secret," he explains. "We're looking for the best quality risk and the price of insurance reflects that risk."

As organizations begin to scale, particularly digitally, security risk increases. "What would have been ok three or five years ago isn't ok today because now you have more to lose," says David. "Those companies that have been diligent about protecting their environment by investing in cyber resilience are generally treated more favorably by the insurance market. Those that have neglected security investments may get smacked down."

For example, when organizations grow business functions, again particularly digitally, they may not decide to or may not be able to hire IT staff, which means that the same number of people are stressed to manage a broader, more diverse range of IT operations and security. They may not be able to perform at the same level. That drives the need for more automation of policy-based access controls.

Companies that are merging or acquiring increase their risk as well. "The technical integration process opens the door to risk and must be carefully managed," David says. In Sara's case, one of the drivers increasing the retailer's risk profile was their expansive use of third parties for manufacturing, distribution, marketing, and IT operations support. "Rapidly growing organizations tend to work with more vendors, partners, and contractors as they expand into new markets and focus on their core business," David explains.

Sam, the IT Administrator at Sara's company, had been thinking for some time about making an investment in enterprise Privileged Access Management. The discussion with Sara cemented the plan and helped secure budget.

Sam was concerned that all the responsibility for securing privileged accounts was on the shoulders of just a few people. Having only one or two people hold the keys to critical resources was too much concentrated risk. PAM removes the burden and provides an intelligent, policy-driven system as backup.

The retailer worked with the team at Delinea to meet their PAM requirements and ultimately selected Delinea Secret Server With Secret Server in place, Sara was able to procure the appropriate insurance policy.

Required:

a. "Our appetite for risk isn't a secret,". Discuss this statement citing the factors that can affect risk appetite at Zurich North America. (10 marks)

b. From the case above, it's evident that risk transfer as a risk strategy has been employed. Discuss the benefits that would accrue to Saras Company as a result of adopting risk transfer (10 marks)

c. The case above exemplifies how risk can occur on the supply chain and its impact on organizational performance. Explain the external sources of supply chain risks that can influence a firm's operations

(10 marks)

Question 2

a. Staff shortages, shipping delays and problems procuring components and materials are all playing their part in preventing businesses from fulfilling their contractual obligations and causing knock-on impacts further down the supply chain.Where delays and disruption to supply chains emerge, contractual disputes inevitably follow, as businesses seek to recoup the losses that result. What are some of the ways of dispute resolution in the case that contractual issues arise because of supply chain disruptions? (10 marks).

b. Globalization is one of the transformational trends influencing the supply chain. What risks does it bring to the supply chain?

(10 marks).

Question 3

a. A supply chain risk strategy contains all the long-term goals, plans, policies, culture, resources, decisions and actions that relate to risks within a supply chain. The main elements of this strategy are usually presented in a written document, which is called a risk policy, strategic plan, management plan or some equivalent title.What are the key aspects included in a risk policy (10marks)

b. What consequences does risk bring to a supply chain?

(10 marks)

Question 4

a. Managers make decisions in very complex circumstances – with rapidly changing conditions, and, diverse stakeholders. List some of the key stakeholders for organizations and the risk they bring to organizational operations (10 marks)

b. Effective supplier selection could be one of the ways to mitigate risk along the supply chain. What are the factors to consider in the supplier appraisal and selection process?

(10 marks)

Question 5

a) How can technology be used as a protective factor against risk along the supply chain

(10 marks)

b) There are specific ways ofdealing with risks, involving both the design of supply chains and theway that the flow of materials is controlled. What are some of the available options for supply chain risk managers to deal with risks?

(10 marks)