

## **BCRM'25 | Project**

### **Milestone 1**

#### **Grade (20)**

#### **Problem Description:**

In today's rapidly evolving digital landscape, organizations face an increasing number of cyber threats that can compromise sensitive data, disrupt operations, and damage reputations. Risk management plays a crucial role in identifying, assessing, and mitigating potential security risks before they lead to significant harm. By implementing a structured risk management framework, organizations can develop proactive strategies to protect their assets, ensure business continuity, and comply with regulatory requirements. In cybersecurity, frameworks like OCTAVE Allegro provide a systematic approach to risk assessment, ensuring that organizations make informed decisions about security investments and incident response strategies.

#### **Required**

1- Each group should choose one of the following systems:

- **System 1: Securing a University's Online Learning Platform.**
- **System 2: Strengthening Security in a University's Cloud Storage System.**
- **System 3: Enhancing Security of a Smart Campus Network.**
- **System 4: Securing a Healthcare System in a University Hospital.**
- **System 5: Cybersecurity Risk Assessment for a University's Financial Services.**

2- Apply OCTAVE Allegro Risk Assessment Framework to the chosen system for:

- Defining information assets.
- Identifying potential threats.
- Ranking risks based on operational, reputational, and compliance impact.
- Suggesting mitigation techniques.

## **BCRM'25 | Project**

### **Milestone 2**

#### **Grade (20)**

#### **Problem Description:**

In an increasingly digital and interconnected world, organizations face various risks that can disrupt operations, compromise critical assets, and impact financial stability. Business Impact Analysis (BIA) is a fundamental process that helps organizations identify and assess the potential consequences of disruptions to their key operations, services, and systems.

#### **Required**

Based on the system that has been chosen in Milestone 1, Apply BIA using a weighted analysis table for:

- Identifying Critical Business Assets.
- Set appropriate recovery priorities through **Weight Analysis Table**.
- Defining RTOs and RPOs for restoration of affected systems.

## **BCRM'25 | Project**

### **Milestone 3**

#### **Grade (20)**

#### **Problem Description:**

In the ever-evolving cybersecurity landscape, organizations face a variety of cyber threats that can compromise their systems, disrupt operations, and cause financial or reputational damage. To effectively mitigate risks, security teams must develop an Attack Profile and conduct a Potential Damage Assessment, which helps them understand how attackers operate and the extent of harm a successful attack could cause.

An Attack Profile involves identifying potential threat actors, their motives, tactics, techniques, and procedures (TTPs) based on real-world attack patterns.

#### **Required**

Based on the system that has been chosen in Milestone 1 and Milestone 2, Build an attack profile & potential damage assessment by:

- Identify attack vectors.
- Analyze the motivation and capabilities of potential attackers.
- Assess the potential for damage.
- Recommend countermeasures

**Instructions (For All Milestones):**

- 1) Teams can have 5 members at most.
- 2) Teams for all Milestones are the same.
- 3) The deadline for submitting all Milestones will be 24 April.
- 4) The discussion will start from 30 April onwards.

**Deliverable:**

<https://docs.google.com/forms/d/e/1FAIpQLScE9Fx1wxNiEfvwRQel3vLNTzUVGp-H53VdqIeIR6Bkid8O4Q/viewform?usp=sharing>