Assessing Risks and Mitigation Strategies: A Study of Felicity

- **Overview:**
  Felicity, IIIT Hyderabad's annual college fest, is a vibrant celebration of creativity, talent, and innovation. It gathers students from various backgrounds to showcase skills and compete in a supportive atmosphere.
- **Threats:**
  1. Physical Security Threats:
     - Large gatherings can lead to overcrowding and potential stampedes, especially during peak times or popular events. Inadequate crowd control measures can result in injuries.
     - Unrestricted access to event venues can lead to various security breaches, including theft or unauthorized entry into restricted areas.
  2. Logistical Threats:
     - Technical equipment such as sound systems, lighting, or AV equipment may malfunction during the event, leading to disruptions or delays.
     - logistical risks related to vendor reliability, performance, or contractual issues.
  3. Cybersecurity Threats:
     - Technological infrastructure used in events, such as online ticketing systems or attendee databases, may be vulnerable to hacking or data breaches.
  4. Environmental Threats:
     - Outdoor events are vulnerable to adverse weather conditions such as rain, storms, or extreme temperatures, which can disrupt event activities and compromise attendee safety.
  5. Safety Threats:
     - Fire hazards such as electrical faults, flammable materials, or overcrowded exits pose significant risks to event safety.
     - Improper electrical installations or overloaded circuits can lead to electrical fires, shocks, or equipment malfunctions.
  6. Security Threats:
     - Some people might get offended by the program content and might pose security risk to the event by causing harm through acts of violence.
  7. Health related Threats:
     - Students might fell sick due to various reasons.
- **Threat Agents:**
  - Unruly attendees, individuals attempting to breach security checkpoints
  - Attendees experiencing health crises, such as injuries, heatstroke
  - Hackers or cybercriminals seeking to exploit vulnerabilities in event websites, databases, or payment systems to steal personal information or financial data.
  - Unreliable vendors, subcontractors, or service providers
  - External factors such as transportation delays, manufacturing issues, or natural disasters

  - Accidental ignition sources, faulty electrical wiring, or flammable materials contributing to fire incidents
  - Poorly maintained electrical systems, overloaded circuits, or non-compliance with safety standards leading to electrical fires or shocks
  - Extremist groups, disgruntled individuals
  - Rain or extreme heat
- **Vulnerability:**
  - Vulnerable entry points, insufficient barriers, inadequate crowd management strategies
  - Weak perimeter security, lack of surveillance coverage, poorly secured access points
  - Inadequate medical staff or facilities, lack of emergency response protocols, insufficient medical supplies
  - Unencrypted sensitive data, outdated software or security patches, weak authentication mechanisms
  - Lack of equipment maintenance, inadequate backup systems, reliance on single suppliers
  - Insufficient vendor screening, vague contractual agreements, lack of contingency plans for vendor failures
  - Inadequate fire detection and suppression systems, blocked emergency exits, improper storage of flammable materials
  - failure to recognize suspicious behaviour
  - Not monitoring weather forecasts
- **Risks:**
  - Risk of stampedes, trampling, or injuries due to overcrowding
  - Risk of theft, delayed or inadequate medical response to emergencies
  - Risk of compromised personal or financial information, leading to identity theft or fraud
  - Risk of disruption to event operations, data loss, or financial losses
  - Risk of interruptions to event activities or performances, Risk of service disruptions or subpar service quality
  - Risk of property damage, injuries, or fatalities in the event of a fire. Risk of electrical fires, shocks, or equipment damage
  - Risk of event disruption, property damage, or attendee safety hazards due to severe weather conditions
- **Impact Analysis:**
  - High Impact: Risks with significant consequences that could severely affect the event, attendees, or stakeholders. This may include risks that result in substantial financial losses, injuries, fatalities, or reputational damage. Crowd control, violence, data breach, fire hazard,
  - Medium Impact: Risks with moderate consequences that could cause disruptions to event operations, inconvenience to attendees, or moderate financial losses. This

may include risks that result in minor injuries, property damage, or temporary closures. Weather related issues, equipment failure

- Low Impact: Risks with minimal consequences that have limited impact on the event, attendees, or stakeholders. This may include risks that result in minor disruptions, negligible financial losses, or inconveniences to a small number of attendees. Temporary power outage, minor technical glitches in audiovisual equipment, or brief interruptions in scheduled activities

- **Likelihood Analysis:**
  - High likelihood: Crowd control, Environmental Threats, Trespassing and Unauthorized Access
  - Medium likelihood: Medical Emergencies, Equipment Failure, Fire Hazards, Electrical Hazards
  - Low likelihood: Data Breaches, Vendor Management, Supply Chain Disruptions
- **Incidents:**
  - Events planned in afternoon delayed due to heat
  - Many students not feeling well.