1. Streamline those into assets, threats, vulnerabilities, and controls

#### **Incident 1: Data Leak Incident**

* Asset: Data Storage and Management Systems (Sensitive company and customer information)
* Threat: Cyberattacks (Hackers targeting data storage systems)
* Vulnerability: Inadequate Cybersecurity Measures (Lack of robust firewalls and intrusion detection systems)
* Control:
  + Implement robust firewalls and intrusion detection systems
  + Conduct regular security audits and vulnerability assessments
  + Provide continuous training for employees on data protection and cybersecurity practices

#### **Incident 2: System Downtime Due to Cyberattack**

* Asset: Network Infrastructure (Servers and network devices)
* Threat: Cyberattacks (Distributed Denial-of-Service (DDoS) attacks)
* Vulnerability: Inadequate Cybersecurity Measures (Insufficient DDoS protection)
* Control:
  + Deploy DDoS protection services
  + Monitor network traffic for unusual patterns
  + Develop an incident response plan to quickly mitigate attacks

#### **Incident 3: GPS System Hacked**

* Asset: IT Systems (GPS tracking system)
* Threat: Cyberattacks (Hackers exploiting software vulnerabilities)
* Vulnerability: Software Maintenance (Failure to regularly update and secure software)
* Control:
  + Ensure regular software updates and patches
  + Conduct security assessments on the GPS system
  + Implement strong encryption protocols for data transmission

#### **Incident 4: Unauthorized Access to Fleet Management System**

* Asset: IT Systems (Fleet management system)
* Threat: Cyberattacks (Unauthorized access to IT systems)
* Vulnerability: Weak Authentication Protocols (Use of weak passwords and lack of multi-factor authentication)
* Control:
  + Enforce strong, unique passwords
  + Implement multi-factor authentication (MFA) for all system access points
  + Regularly review and update authentication protocols

1. Apply the quantitative method to do the CBA

**Scenario**

Consider a transportation company that wants to evaluate the financial impact of GPS software is faulty.

**Single Loss Expectancy (SLE)**

* Asset Value (AV): The value of a single software in each truck is $1000.
* Exposure Factor (EF): The percentage of loss that would occur if the truck or software has problem. Let's assume it’s 100% is a total loss.

**SLE = AV x EF**

**= $1000 x 1**

**= $1000**

**Annual Rate of Occurrence (ARO)**

Software updates in 1 year are about 5 times.

**ARO** **= 5**

**Annual Loss Expectancy (ALE)**

**ALE = SLE x ARO**

**= $1000 x 5**

**= $5000**

1. Apply the qualitative method to prioritize the risk & the control

**-** In the qualitative method, we prioritize risks and controls based on their impact and likelihood, using a risk matrix or risk assessment framework.

**Risk Assessment**

* Impact: High (Faulty GPS software can lead to significant operational inefficiencies and potential loss of assets).
* Likelihood: Medium (Faults occur 5 times a year).
* Given the high impact and medium likelihood, this risk falls into the high-priority category.

**Control Prioritization**

* Implement robust GPS software update system: High priority due to significant reduction in ARO and positive net benefit.
* Regular software testing and maintenance: Medium priority to ensure software is functioning correctly.