# ISO / IEC 27001:2022 Lead Implementer Course


## Exercise 20:

**Instructions:**

- Prepare a Risk Treatment Plan
- Consider first writing the risk methodology and combine it with the risk treatment
- Considering your company as a case study for ISO 27001:2022 implementation
- Take a blank piece of a white paper, write (by-hand). Do not copy or review; trust your memory.
- Take a clear snapshot of the paper, create a folder on Google Drive 'ISO 27001:2022 Lead' and save the snapshot (If you did not create in Exercise A)
- Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
- Facebook link: facebook.com/profile.php?id=61556175711538

Follow me on my social media platforms to learn more about ISO / IEC 27001:2022 via my posts:

- LinkedIn: linkedin.com/in/john-kimani-13831329b
- Facebook: facebook.com/profile.php?id=61556175711538
- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary

# Risk Treatment Plan for Stoopid Boy Animations Inc:

## Objective:-

To identify, assess, and treat risk that may impact the Information Security Management System (ISMS) of Stoop Boy Animations Inc. in Compliance with ISO 27001:2022 standards.

## Risk Assessment Methodology

### 1. Risk Identification:-

- Assets: Identify all information assets such as data, software hardware and personnel
- Threats :- Determine potential threats to each asset (e.g cyber-att natural disasters, human error)
- Vulnerabilities :- Identify Vulnerabilities that could be exploited threats (e.g outdated software, lack of employee training)

### 2. Risk Analysis:-

- Impact; Assess the potential impact of each threat on the Organized assets.
- Likelihood :- Determine the probability of each threat occuring
- Risk Level :- Calculate the risk level by Combining the impact and likelihood using a risk matrix (e.g Low, Medium, High)

### 3. Risk Evaluation:-

- Compare the identified risk levels against the Organizations risk appetite and tolerance
- Prioritize risk based on their levels to decide which requires immediate attenti

### 4. Risk Treatment Options:-

- Avoidance :- Eliminate the risk by discontinuing the activity that generates it
- Mitigation:- Implement measures to reduce the likelihood or impact of the risk
- Transfer:- Shift the risk to a third party (e.g through insurance or Outsourcing
- Acceptance:- Acknowledge the risk and decide to accept it without additional

# Risk Treatment Plan

## 1. Risk Treatment Measures

- **Data Breach:**
  - Mitigation:- Implement encryption for sensitive data, conduct regular security audits, and provide employee on data protection
  - Transfer:- Obtain cyber insurance to cover potential data breach cost

- **Ransomware Attack:-**
  - Mitigation:- Install and regularly update anti-malware Software Create regular backups, and establish a robust incident response plan.

- **Natural Disasters:-**
  - Avoidance:- Relocate critical servers to areas less prone to natural disasters.
  - Mitigation:- Develop and test a disaster recovery plan, and ensure off-site backups are maintained.

- **Human Error:-**
  - Mitigation:- Conduct regular training sessions for employees on information security best practices and implement automated systems to minimize manual errors.

- **Outdated Software:-**
  - Mitigation:- Establish a patch management policy to ensure all software is updated.

## 2. Implementation Plan:-

- Assign responsibilities for each treatment to measure to appropriate personnel
- Set deadlines for the implementation of each measure
- Allocate necessary resources (financial, technological and human) to