ISO / IEC 27001:2022 Lead Implementer Course

Exercise 12:

Instructions:

- Write your risk Assessment Methodology
- 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 Assessment Methodology for Stoopid Boy Animations Inc:

1. Identify Assets:-
   - List all information assets (e.g. hardware, Software, data, people)

2. Identify Threats and Vulnerabilities:-
   - Determine potential threats (e.g., Cyber-attacks, natural-disasters)
   - Identify Vulnerabilities in assets (e.g, outdated Software, weak passwo

3. Assess Impact and Likelihood:-
   - Evaluate the potential impact of each threat on asset (e.g., data loss, service interruption).
   - Determine the likelihood of each threat occurring (e.g. high, medium, low).

4. Calculate Risk:-
   - Use a risk formula:- Risk = Impact x Likelihood.
   - Prioritize risks based on their Calculated Values.

5. Mitigation Measures:-
   - Identify and implement Controls to mitigate high-priority risks (e.g. firewalls, employees' training).

6. Review and Update:-
   - Regularly review and Update the risk assessment to account for new assets, threats and Vulnerabilities.

7. Documentation:-
   - Document all steps, findings and actions taken for transparency and future reference.