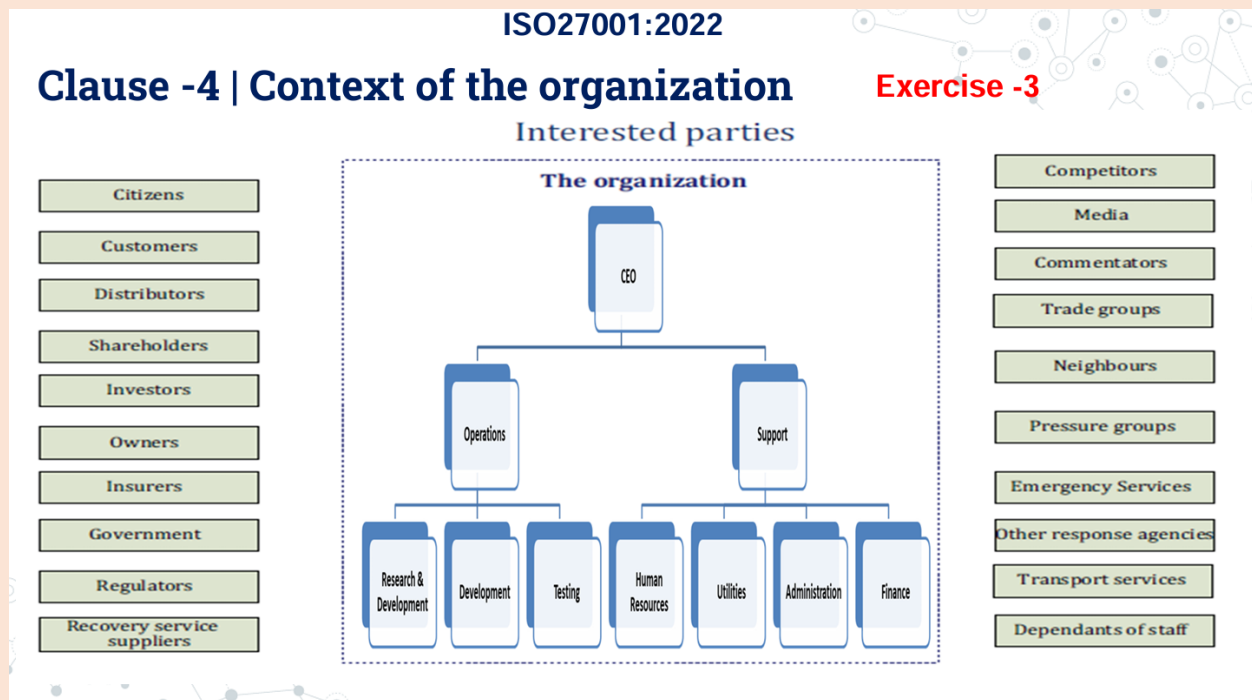# ISO / IEC 27001:2022 Lead Implementer Course

Exercise 3:

1) Use the sample below
2) List down the interested parties
3) List down their issues based on ISO 27001:2022
4) Consider your company as a case study for ISO 27001:2022 implementation
5) This exercise is complex and can take weeks
6) Take a blank piece of a white paper, write (by-hand) the interested parties and issues. Do not copy or review; trust your memory.
7) 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)
8) Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
9) Facebook link: facebook.com/profile.php?id=61556175711538

Sample:

ISO27001:2022

Clause -4 | Context of the organization   Exercise -3

Interested parties

The organization

CEO

Operations | Support

Research & Development | Development | Testing | Human Resources | Utilities | Administration | Finance

Citizens
Customers
Distributors
Shareholders
Investors
Owners
Insurers
Government
Regulators
Recovery service suppliers

Competitors
Media
Commentators
Trade groups
Neighbours
Pressure groups
Emergency Services
Other response agencies
Transport services
Dependants of staff

Below is my snapshot:

Stoopid Boy Animations Inc.
Cl - 4 :- Context of the Organization.

Company :-
Stoopid Boy Animations Inc.

Interested Parties & Their Needs :-
1. Employees (Contractors, Staff and Freelancers)
   Needs :-
   - Secure and reliable access to information & resources.
   - Protection of personal and professional data.
   - Clear policies and Security awareness training.
2. Customers & Clients.
   Needs :-
   - Assurance that their data, Intellectual properties & Personal information is pro
   - Reliable and Secure services with minimum disruption.
   - Transparency regarding data handling and security practices
3. Shareholders and Investors
   Needs :-
   - Confidence in the ability that the company can protect it's assets & reputation.
   - Assurance that information Security risks are effectively managed
   - Regular updates on the Company's information security posture and Inciden
   Response.
4. Regulatory Bodies and Compliance Authorities.
   Needs :-
   - Compliance with relevant information security laws and regulations
   - Documentation and evidence of effective Information Security Managemen
   - Regular audits and assessment to ensure ongoing compliance
5. Suppliers and Vendors
   Needs
   - Protection of Shared intellectual property and Sensitive information.
   - Assurance of Secure Collaboration platforms and practices
   - Clear guidelines and agreements on information security responsibilities

6. Business Partners and Collaborators

Needs

- Protection of shared intellectual property and sensitive information
- Assurance of secure collaboration platforms and practices
- Clear guidelines and agreements of information security responsibilities

7. End Users (Viewers and Consumers of content)

- Protection of their personal data and privacy
- Secure and reliable access to content and services
- Assurance and their interaction with the company is secure

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