

# ISO / IEC 27001:2022 Lead Implementer Course

## Exercise 4:

### Activity A Instructions:

- From the sample below; create your own list (Interested parties / needs & expectations)
- Consider 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](https://facebook.com/profile.php?id=61556175711538)



### Sample:

## Clause -4 | Context of the organization

### Exercise -4

#	Interested Parties	Need & Expectations (Requirements)
1	Business Owners- INFOCUS-IT	<ul style="list-style-type: none"><li>• To Safeguard Confidential, Restricted and Internal information against unauthorized disclosure/Misuse.</li><li>• Focus on continuous strengthening of information security strategies</li><li>• The trade secrets should be kept limited to authorized personnel only</li><li>• To ensure correct and secure operations of information processing facilities.</li><li>• Business Facility protection against natural disasters, malicious attack or accidents</li><li>• Compliance w.r.t. to all legal requirements as per the requirement of the standard ISO27001.</li></ul>
2	Employees	<ul style="list-style-type: none"><li>• Awareness of Information Security / ISO27001 for INFOCUS-IT</li><li>• Resource availability to comply Information Security / ISO27001 INFOCUS-IT Policy</li><li>• Privacy and protection of personally identifiable Information</li></ul>
3	Customers	<ul style="list-style-type: none"><li>• Information security aspects of business continuity management.</li><li>• Management of information security incidents and improvements</li></ul>
4	Suppliers /Vendors / Service Providers	<ul style="list-style-type: none"><li>• Robust information security systems to support business transactions with supported Service Level Agreement.</li></ul>
5	Legal and Regulatory Bodies	<ul style="list-style-type: none"><li>• Complaisance of applicable Legal and Statutory guidelines/procedure.</li></ul>
6	Banking, financial Institutions & Business Forums	<ul style="list-style-type: none"><li>• To Avoid fraudulent nature of transactions and safeguard organization business data from cyber Breach</li></ul>

## 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 protected.
- 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 its assets & reputation.
- Assurance that information security risks are effectively managed.
- Regular updates on the company's information security posture and Incident Response.

#### 4. Regulatory Bodies and Compliance Authorities.

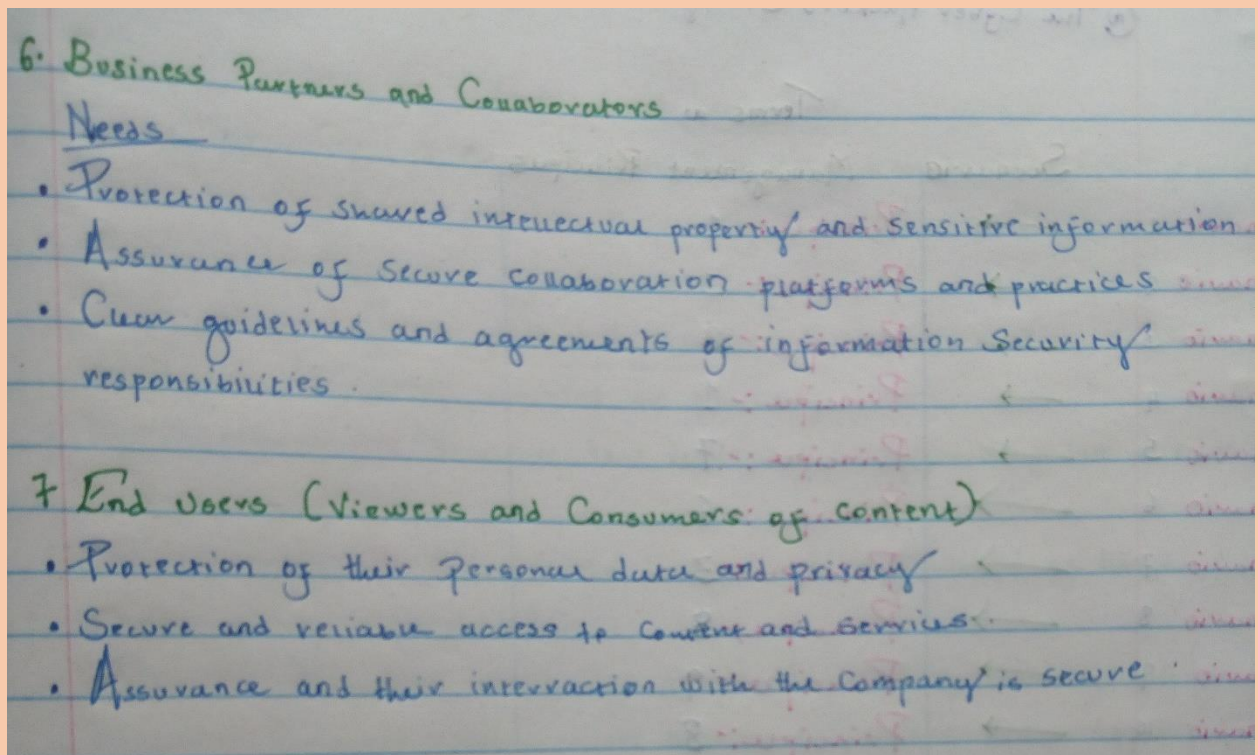
Needs :-

- Compliance with relevant information security laws and regulations.
- Documentation and evidence of effective Information Security Management.
- 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.



### Activity B Instructions:

- Fill in the table below
- 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](https://facebook.com/profile.php?id=61556175711538)

## Clause -4 | Context of the organization

### 4.1 Understanding the organization and its context

Information (Assets)	People	Organization	Product/Services	Systems/Process
----------------------	--------	--------------	------------------	-----------------



## My snapshot:

Stoopid Boy Animations Inc.  
Understanding the Organization & its Context.

Information Assets	People	Organization	Product/Service	Systems/Process
① Sensitive Animation Files	Employees	Business Partners	Animation Content	IT Infrastructure
② Customer data	Customers	Investors	Customer Support	Content Management systems
③ Intellectual Property	Board of directors	Regulatory Bodies	Licensing & distribution	Security Protocols
④ Financial Records	Suppliers & Vendors	Legal advisors	Merchandise	Incident Response Plan/process
⑤ Contracts & Agreements	Freelancers & Contractors	Competitors	Event participation	Data backup procedures & recovery
⑥ Employee records	IT staff	Community & Fans	Training & Consultancy	Network Security Controls
⑦ Marketing Strategies	Security Personnel	Media	Digital Platform Services	Access Control policies
⑧ Proprietary Software & tools	Auditors	Standards Organizations	Online Streaming	Software Dev. Lifecycle

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