ISO / IEC 27001:2022 Lead Implementer Course

Exercise 21:

Instructions:

- Create a Statement of Applicability (SOA) for your organization
- 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

Statement of Applicability (SOA) for Stoopid Boy Animations Inc.

Purpose:-

To provide an overview of selected controls to mitigate risks in compliance with ISO/IEC 27001:2022.

Scope:-

Covers all information assets, processes, and systems with Stoopid Boy Animations Inc.

Control Objectives and Controls.

- A.5 Information Security Policies
- Management direction for Information Security:- yes

- A.6 Organization of Information Security.
- Roles and responsibilities :- yes
- Mobile device and teleworking :- yes.

- A.7 Human Resource Security.
- Background checks :- yes
- Awareness training :- yes.

- A.8 Asset Management.
- Asset Inventory :- yes
- Information classification :- yes.

- A.9 Access Control
- Restrict access to authorized users :- yes
- User registration process :- yes.

- A.10 Cryptography.
- Cryptographic Controls policy :- yes.

- A.11 Physical and Environmental Security
- Physical Security perimeters :- yes

- A.12 Operations Security :
  Documented Operating procedures :- yes

- A.13 Communications Security :
- Network Security Management :- yes

- A.14 System Acquisition, Development, and Maintenance :
- Security requirements in Systems : yes

- A.15 Suppliers Relationships
  Supplier security agreements :- yes

- A.16 Information Security Incident Management :
- Incident Management procedures :- yes

- A.17 Information Security Aspect of Business Continuity Man
- Information Security Continuity :- yes

- A.18 Compliance
- Legal and Contractual Compliance :- yes