

ISO / IEC 27001:2022 Lead Implementer Course

Exercise 1:

- 1) Go through Clause 1, Clause 2 & Clause 3
- 2) We have two categories in this exercise:
 - Terms (1-15)
 - Definition / Standard terms (A-O)
- 3) Match the Definitions / Standards with the term that suits best
- 4) Take a blank piece of a white paper, write (by-hand) the matches. Do not copy or review; trust your memory.
- 5) 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)
- 6) Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
- 7) Facebook link: facebook.com/profile.php?id=61556175711538



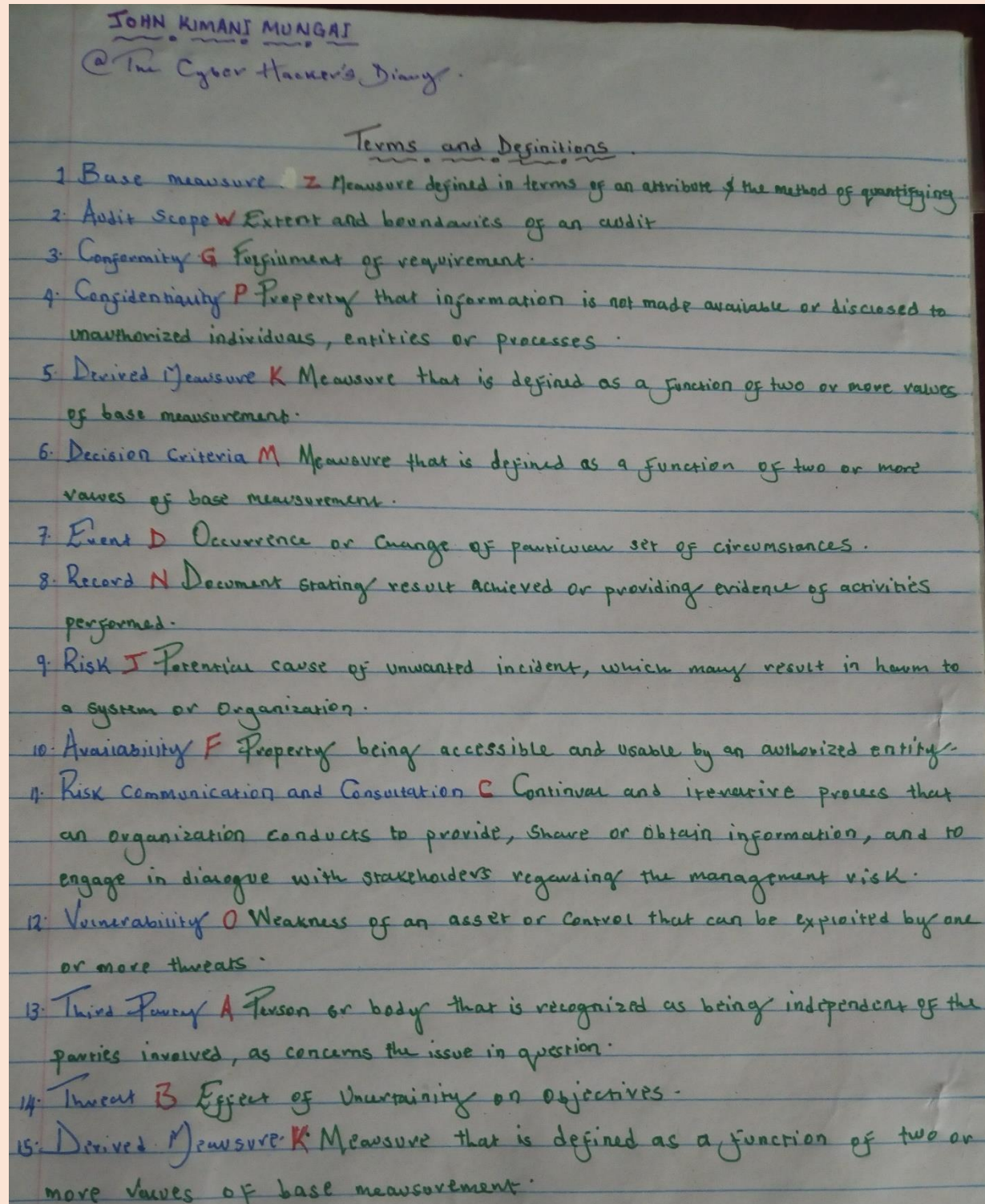
ISO27001:2022

Clause -3 | Terms and definitions

Exercise-1

Term	Definition / Standard Terms
1. Base measure	A Person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
2. Audit scope	B Effect of uncertainty on objectives.
3. Conformity	C Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.
4. Confidentiality	D Occurrence or change of particular set of circumstances.
5. Derived measure	F Property being accessible and usable by an authorized entity.
6. Decision criteria	P Property that information is not made available or disclosed to unauthorized individuals, entities or processes.
7. Event	G Fulfillment of requirement.
8. Record	K Measure that is defined as a function of two or more values of base measures.
9. Risk	W Extent and boundaries of an audit.
10. Availability	J Potential cause of an unwanted incident, which may result in harm to a system or organization
11. Risk communication and consultation	M Measure that is defined as a function of two more values of base measures.
12. Vulnerability	I Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
13. Third party	Z Measure defined in terms of an attribute and the method for quantifying it.
14. Threat	N Document stating result achieved or providing evidence of activities performed.
15. Derived measure	O Weakness of an asset or control that can be exploited by one or more threats.

Below is my snapshot:



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
- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary