# 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	
1. Base measure	
2. Audit scope	
3. Conformity	
4. Confidentiality	
5. Derived measure	
6. Decision criteria	
7. Event	
8. Record	
9. Risk	
10. Availability	
11. Risk communication and consultation	
12. Vulnerability	
13. Third party	
14. Threat	
15. Derived measure	

Definition / Standard Terms  A Person or body that is recognized as being independent of the parties involved, as concerns the issue in question.  B Effect of uncertainty on objectives.  C Continual and iterative processes that an organization conduct provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.  D Occurrence or change of particular set of circumstances.	•
B Effect of uncertainty on objectives. C Continual and iterative processes that an organization conduct provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.	••
Continual and iterative processes that an organization conduct provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.	
provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.	
Occurrence or change of particular set of circumstances.	
F Property being accessible and usable by an authorized entity.	
P Property that information is not made available or disclosed to unauthorized individuals, entitles or processes.	
G Fulfillment of requirement.	
K Measure that is defined as a function of two or more values of base measures.	
W Extent and boundaries of an audit.	
J Potential cause of an unwanted incident, which may result in h to a system or organization	arm
M Measure that is defined as a function of two more values of bar measures.	se
Means of managing risk, including policies, procedures, guidelin practices or organizational structures, which can be of administrative, technical, management, or legal nature.	nes,
Z Measure defined in terms of an attribute and the method for quantifying it.	
N Document stating result achieved or providing evidence of activities performed.	
<ul> <li>Weakness of an asset or control that can be exploited by one o more threats.</li> </ul>	r



# **Below is my snapshot:**

JOHN KIMANI MUNGAI
@ The Cyber Hacker's Diany.
Terms and Desinitions.
1 Base meansure. I Meansure defined in terms of an attribute of the method of quantifying.
Addit Scope w Extent and boundaries of an audit
3. Conformity & Forginment of requirement.
4. Consider having P Property that information is not made available or discussed to
mathemata individuals, entitles or processes.
5 Derived Meansure K Meansure that is defined as a function of two or more values.
of gase meansurement.
6. Decision Criteria M Meansure that is defined as a function of two or more
valves of base meansurement.
7. Event D Occurrence or Change of pourievan set of circumstances.
8. Record N Document stating result achieved or providing evidence of activities
performed.
9. Risk J Perential cause of unwanted incident, which many result in how to
a system or Organization.
10. Availability F Property being accessible and usable by an authorized entity
1. Risk communication and Consulation C Continuou and iterative process that
an organization conducts to provide, Shave or Obtain information, and to
engage in dialogue with stakeholders regarding the management visk.
12. Vunerability O Weakness of an asset or control that can be exploited by one
or more threats.
13. Third Penny A Person or body that is recognized as being independent of the
parties involved, as concerns the issue in question.
14. Threat B Egger of Unarrainity on Objectives.
15. Derived Mewsure K Meausure that is defined as a function of two or
more values of base meansovement.

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