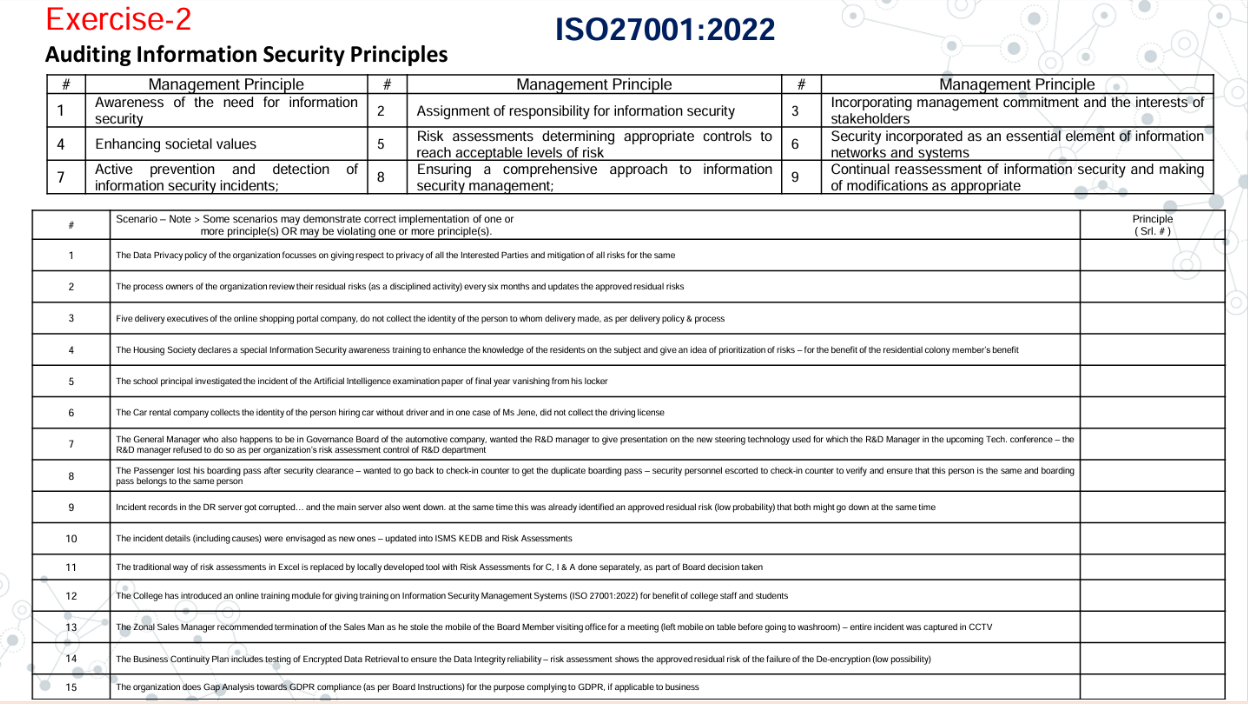
ISO / IEC 27001:2022 Lead Implementer Course

Exercise 2:

1) Go through Clause 1, Clause 2 & Clause 3
2) We have two categories in this exercise:
- Management Principle(s) (1-9)
- Case scenarios (1-15)
3) Match the scenarios with the management principle 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



Exercise-2

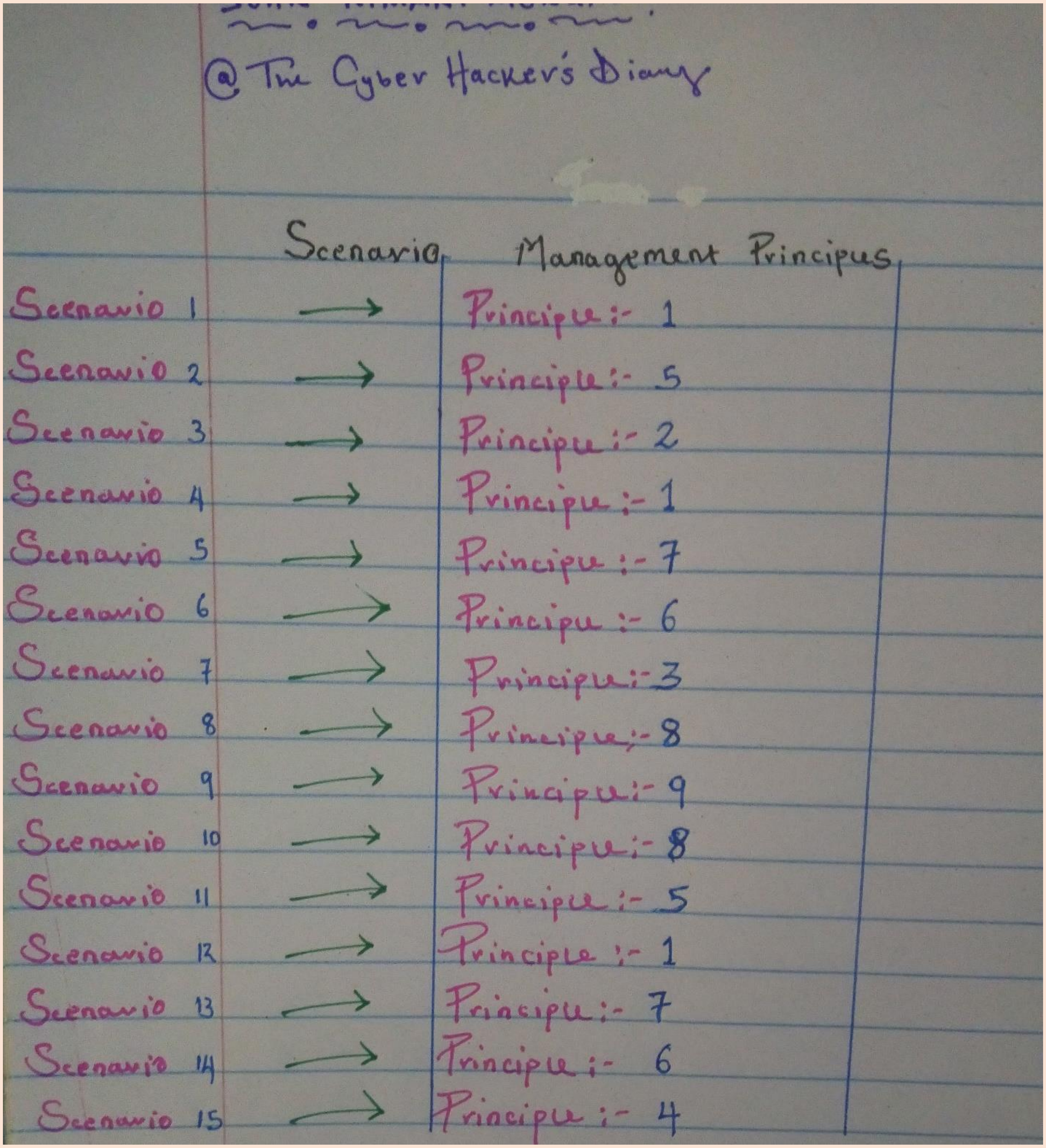
ISO27001:2022

Auditing Information Security Principles

#	Management Principle	#	Management Principle	#	Management Principle
1	Awareness of the need for information security	2	Assignment of responsibility for information security	3	Incorporating management commitment and the interests of stakeholders
4	Enhancing societal values	5	Risk assessments determining appropriate controls to reach acceptable levels of risk	6	Security incorporated as an essential element of information networks and systems
7	Active prevention and detection of information security incidents;	8	Ensuring a comprehensive approach to information security management;	9	Continual reassessment of information security and making of modifications as appropriate

#	Scenario – Note > Some scenarios may demonstrate correct implementation of one or more principle(s) OR may be violating one or more principle(s).	Principle (Srl. #)
1	The Data Privacy policy of the organization focusses on giving respect to privacy of all the Interested Parties and mitigation of all risks for the same	
2	The process owners of the organization review their residual risks (as a disciplined activity) every six months and updates the approved residual risks	
3	Five delivery executives of the online shopping portal company, do not collect the identity of the person to whom delivery made, as per delivery policy & process	
4	The Housing Society declares a special Information Security awareness training to enhance the knowledge of the residents on the subject and give an idea of prioritization of risks – for the benefit of the residential colony member's benefit	
5	The school principal investigated the incident of the Artificial Intelligence examination paper of final year vanishing from his locker	
6	The Car rental company collects the identity of the person hiring car without driver and in one case of Ms Jene, did not collect the driving license	
7	The General Manager who also happens to be in Governance Board of the automotive company, wanted the R&D manager to give presentation on the new steering technology used for which the R&D Manager in the upcoming Tech. conference – the R&D manager refused to do so as per organization's risk assessment control of R&D department	
8	The Passenger lost his boarding pass after security clearance – wanted to go back to check-in counter to get the duplicate boarding pass – security personnel escorted to check-in counter to verify and ensure that this person is the same and boarding pass belongs to the same person	
9	Incident records in the DR server got corrupted… and the main server also went down. at the same time this was already identified an approved residual risk (low probability) that both might go down at the same time	
10	The incident details (including causes) were envisaged as new ones – updated into ISMS KEDB and Risk Assessments	
11	The traditional way of risk assessments in Excel is replaced by locally developed tool with Risk Assessments for C, I & A done separately, as part of Board decision taken	
12	The College has introduced an online training module for giving training on Information Security Management Systems (ISO 27001:2022) for benefit of college staff and students	
13	The Zonal Sales Manager recommended termination of the Sales Man as he stole the mobile of the Board Member visiting office for a meeting (left mobile on table before going to washroom) – entire incident was captured in CCTV	
14	The Business Continuity Plan includes testing of Encrypted Data Retrieval to ensure the Data Integrity reliability – risk assessment shows the approved residual risk of the failure of the De-encryption (low possibility)	
15	The organization does Gap Analysis towards GDPR compliance (as per Board Instructions) for the purpose complying to GDPR, if applicable to business	

Below is my snapshot:



@The Cyber Hacker's Diary

	Scenario	Management Principles
Scenario 1	→	Principle :- 1
Scenario 2	→	Principle :- 5
Scenario 3	→	Principle :- 2
Scenario 4	→	Principle :- 1
Scenario 5	→	Principle :- 7
Scenario 6	→	Principle :- 6
Scenario 7	→	Principle :- 3
Scenario 8	→	Principle ;- 8
Scenario 9	→	Principle :- 9
Scenario 10	→	Principle :- 8
Scenario 11	→	Principle :- 5
Scenario 12	→	Principle :- 1
Scenario 13	→	Principle :- 7
Scenario 14	→	Principle :- 6
Scenario 15	→	Principle :- 4

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