

ACTIVITY 1:

1. Matching activity- Match the Term with its definition:

Term	Definition
1. ISO 27001	A. The process of identifying and assessing risks to information.
2. Information Security Management System (ISMS)	B. The core set of policies, procedures, and systems for securing information.
3. Risk Assessment	C. An international standard for information security management.
4. Security Controls	D. A framework of 114 controls to improve information security.
5. Compliance	E. The process of adhering to legal, regulatory, and contractual security requirements.
6. Trust	F. The confidence that customers and partners have in an organization's ability to protect data.
7. Efficiency	G. The ability to manage risks and avoid costly security incidents.
8. Reputation	H. The positive public image organizations gain from following ISO 27001 standards.
9. Certification	I. The process of undergoing an external audit to verify compliance with ISO 27001.

True or False Activity

2. Read the following statements based on the text "What is ISO 27001? A Standard to Protect Information" and mark them as True (T) or False (F):

- ISO 27001 is only applicable to large organizations.
- The core of ISO 27001 is the Information Security Management System (ISMS).
- Risk assessment is optional when implementing ISO 27001
- ISO 27001 includes a list of 114 security controls grouped into 14 categories.
- Compliance with ISO 27001 ensures organizations meet all cybersecurity requirements, including legal and regulatory ones.
- Trust is one of the benefits of implementing ISO 27001, as it builds confidence with customers and partners.
- Certification for ISO 27001 requires an external audit.
- ISO 27001 is specifically designed for IT companies and not other industries
- Organizations certified in ISO 27001 demonstrate a commitment to protecting sensitive information.
- ISO 27001 is a response to the increasing importance of protecting information in the modern digital age.