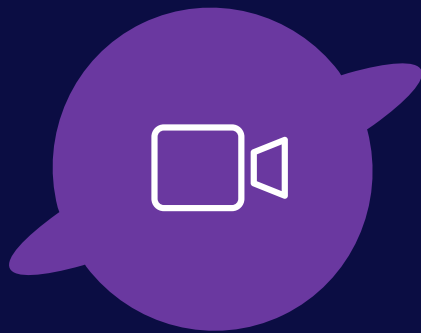




Information Classification ISO 27001:2013

Calculative Measurement in rating your organization documents

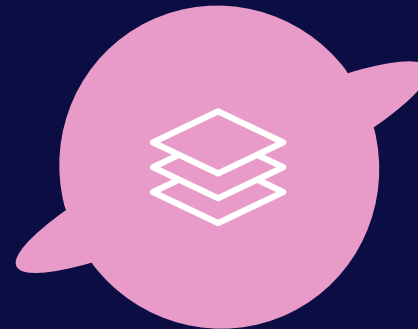
ISO 27001 :2013 Asset Management



8.1 Responsibility of Assets



8.2 Information Classification



8.3 Media Handling



Why are assets important for information security management?

Risk Assessment

- Key element of identifying risks, together with threats and vulnerabilities

Responsibility Assignments

- Defines asset owners
- Assigns owners the responsibility to protect the confidentiality, integrity and availability of the information.



Asset Management Clauses of ISO 27001:2013

8.1

- Responsibility of assets

8.2

- Information Classification

8.3

- Media Handling



8.1 Responsibility of Assets

- To identify organizational assets and define appropriate protection responsibilities

8.1.1 Inventory of assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained

8.1.2 Ownership of assets

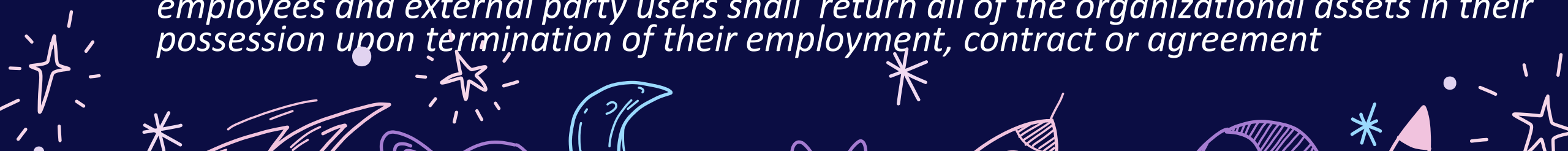
Assets maintained in the Ownership of assets inventory shall be owned

8.1.3 Acceptable use of assets

Rules for acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented

8.1.4 Return of assets

All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement



8.2 Information Classification

- To ensure that information receives an appropriate level of protection in accordance with its importance to the organization

8.2.1 Classification of information

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification

8.2.2 Labelling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with information classification scheme adopted by the organization

8.2.3 Handling of assets

Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization





1

Category

■
Defining & Categorizing



“

“Without knowledge, he who is
confused remains confused”

Information Classification Category

* Information Classification is a process in which organization assess the data that they hold and the level of protection it should be given. Information Classification is derived based on two processes:

* Identifying and labelling of information

* Information Handling Process



Classification is derived from 2 process

CRITICALITY

*Criticality is measured by the dependency on information **AVAILABILITY** to conduct normal operation*

SENSITIVITY

*Sensitivity is defined by information value (**CONFIDENTIALITY** and **INTEGRITY**) that should not be disclosed or can be disclosed with proper authorization.*



Measure

Mechanism to calculate without
playing the guessing game



Information Classification Measurement rating

Rating	Value
Low	1
Medium	2
High	3

Table	Criticality									
	Confidentiality	Low			Medium			High		
	Integrity	L	M	H	L	M	H	L	M	H
Availability	Low	3	4	5	4	5	6	5	6	7
	Medium	4	5	6	5	6	7	6	7	8
	High	5	6	7	6	7	8	7	8	9

Category	Asset Value
Secret	9
Confidential	7-8
Restricted	5-6
Public	3-4

Example

National CyberSecurity Framework is rawSEC business strategy document for 2019 which was just recently tabled to NACSA.

(C)onfidentiality = **HIGH**

(I)ntegrity = **HIGH**

(A)vailability = **MEDIUM**

$$\begin{aligned}
 \text{Category} &= (\text{HIGH}) + (\text{HIGH}) + (\text{MEDIUM}) \\
 &= (3) + (3) + (2) \\
 &= 8
 \end{aligned}$$





**So Let's
Practice**



Trivia Cuestión

Cuestión Uno

Saloma is preparing a User Guideline which must always be available to all users. This document will be placed near the entrance door and in the Online Portal. Define the Document Classification.

Cuestión Dos

Ramlee has just completed developing the department operational procedure document. This document is strictly used within the department to be referenced by its team member for daily operation. Define the Document Classification.

Cuestión Thres

Sudin's department has just completed the external audit exercise. The report was just recently tabled to the audit committee. A follow up and verification is scheduled to be conducted within 3 months time. The audit finding was sent to the respective owners for rectification purposes. Define the Document Classification.



Thanks!

Any questions?

You can find me at:

 @t3kukur

nadzmi@rawsec.com

