

Guideline for People Asset Valuation

Document ID	ISMS/GL/	002	Classification	Internal Use Only
Version Number	Initial		Owner	
Issue Date	07-08-2009		Approved By	



This work is copyright © 2009, [Mohan Kamat](#) and [ISO27k implementers' forum](#), some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum (www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.).

1. Overview

Information is accessed or handled by the people from within the organisation as well as the people related to organisation for business requirements.

It becomes necessary to identify such people from within the organisation as well as outside the organisation who handle the organization's information assets.

The analysis such people, who has access rights to the assets of the organisation, is to be done by Business Process Owner i.e. process / function head.

2. Responsibility

	Responsible	Accountable	Consulted	Informed
Identification and Valuation of Assets	Department / Function Heads	Department / Function Heads	ISMS Forum	Apex Committee

3. Asset Valuation for People asset:

The people assets shall include roles handled by

- a. Employees
- b. Contract Employees
- c. Contractors & his employees

a. Guideline for Confidentiality Requirement

This table provides a guideline to identify the Confidentiality requirements and its link to Classification label.

Confidentiality Requirement	Explanation
Low	The role or third party identified has access limited to information assets classified as 'Public'. Security breach by individual/s whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has access limited to information assets classified as 'Internal' and 'Public'. Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role employee or third party identified has access to all types of information assets including information assets classified as 'Confidential' Or IT Assets classified as 'Critical'. Security breach by individual/s to whom the role is assigned would severely affect the business operations.

b. Guideline for Integrity Requirement

This table provides a guideline to identify the Integrity requirements and its link to Classification label.

Integrity Requirement	Explanation
Low	The role or third party identified has limited privilege to change information assets classified as 'Internal' or 'Public' and the his work is supervised. Security breach by individual/s to whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has privilege to change information assets classified as 'Internal', and 'Public' Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role or third party identified has privilege to change information assets classified as 'Confidential' Or Change the configuration of IT assets classified as 'Critical' Security breach by individual/s to whom the role is assigned would severely affect the business operations.

c. Guideline for Availability Requirement

This table provides a guideline to identify the Availibility requirements and its link to Classification label.

Availability Requirement	Explanation
Low	Unavailability of the individual/s whom the role is assigned would have insignificant affect the business operations.
Medium	Unavailability of the individual/s whom the role is assigned would moderately affect the business operations.
High	Unavailability of the individual/s whom the role is assigned would severely affect the business operations.