

INFORMATION ASSET

Kevin Leung • E-mail: kevinleung@pkf-hk.com

Information asset is referred to as any definable piece of information, deemed as “valuable” to an organization. Every database, document or record can so be defined as part of information asset of an organization and is generated during the flow of business process. A client’s address or a client’s contact number is an example of information asset. Usually, information asset has the following characteristics: -

- It is recognized to have value to an organization.
- It is not easily replaceable without cost, skill, time, resource or a combination of these considerations.
- It forms part of an organization’s corporate identity, without which an organization would lose its competitive edge.
- Data classification would normally be Proprietary, Highly Confidential or even Top Secret.

Information asset grows out of an organization’s business process; however if information is vulnerable to theft or corruption, an organization is subject to severe consequences:

- Loss of exclusive use of information: an organization may lose the maximum benefit of owning information. For example, if your competitors can access your client information, they will take away the ownership benefits.
- Loss of information privacy / confidentiality: an organization’s reputation will be tarnished due to breach of information confidentiality.
- Lack of trust and goodwill: both internal staff and external clients become worried about the data; thus use of information requires checking and rechecking.
- Cost of repair and rebuilding: database needs to be repaired or even rebuilt due to corruption or data loss. Not only is the time accounted for professional workers to locate and fix errors, but also in some cases extra equipment required for the salvage.

In order to protect information asset, an organization can adopt a number of measures:

- Keep information asset protected: internally, ensure only authorized persons can access information asset.
- Keep information asset up-to-date and accurate: by the use of system backups, system logs, audit trails, and control keys can ensure data integrity.
- Information asset management to meet external compliance: it can be achieved by taking part in IT/IS Audit, and proper controls.
- Technical control: by the implementation of “hard-to-guess” passwords, an organization can get better protection of data. Most companies are using username or birthday as passwords that can be easily tackled by hackers.
- Physical security: an organization should set up rules for physical access of workstation or server. Also, access of critical information should be logged. ※