Encryption

In assessing and organization’s encryption policies, the auditor needs to take both the requirements derived from regulatory and statutory foundations together with the risk faced by the organization. Such a risk assessment needs to evaluate the cost of securing the data against the added value from implementing encryption. They should also take the various types of encryption into account. Those organizations that have users accessing internal systems externally via VPN, that run complicated e-commerce applications, that maintain sensitive customer or employee information and those with regulated standards need to ensure that they maintain effective controls over the data.

This requires the implementation of effective encryption policies and processes. The goal of an encryption policy is to encrypt data at the requisite times. For instance, IPSec and SSL provide encryption when data travels across a network but do little to protect data stored on disk or database. Similarly, encrypted fields in a database do nothing to protect information as it is accessed across the network.

Security is not just about the strength of encryption. Although this plays some component in any encryption policy, it needs to be taken into the consideration of the whole. In some cases, ultimate strategies such as the hashing of data may provide a better alternative to encryption.

Any organization needs to be in the process of continually re-evaluating its encryption policies and procedures. As organizations move more towards the implementation of [e-commerce](http://en.wikipedia.org/wiki/E-commerce) systems, distributed networking over the Internet and [wireless networks](http://en.wikipedia.org/wiki/Wireless_networks); they need to become aware of the increased risks that they are facing. , some of the considerations that need to be taken into account include:

 Increased opportunities for theft of intellectual property,

 Disclosure of sensitive information,

 Fraud and other criminal activities,

 Theft of bandwidth, and

 Corruption of information.

It is essential to document all encryption policies and procedures in order to ensure that processes are both created and adhered to. This is essential if either stored or transmitted data is to be protected.

When auditing a system, by the auditor’s role is as to validate the inclusion of controls protecting the data of the organization. To do this, management needs to ensure that an encryption management process as being created. It is the auditor’s role to ensure that management has done this. When assessing the encryption management process, some of the concerns that need to be addressed include:

 Do all accessed to encryption keys require dual control? This is that keys need to be controlled through a process where they are composed of two separate components. No one individual within the organization should be able to access all keys and create new ones.

 Are the private keys maintained on a system that is not accessible to developers or unauthorized users?

 Has the organization’s management made an attestation to the effect that encryption policies ensure data protection at the required level?

 Has the system being tested to ensure that the cost of encrypting the data does not surpass the worth of the information being protected?

Is important to note that all data with a requirement to be maintained over time needs be both encrypted and transported to a remote location for storage. What is commonly forgotten in this process is that encryption is not friendly to data retention. Processes need to be in place to ensure that any degradation of data will not destroy the entire information store. A common issue that has occurred with many organizations is the decay of information on backups that have been stored on serial magnetic media such as tapes. In many forms of encryption that have been used the entire tape is reliant on the whole the tape being valid for decryption. In this event, a single piece flaked ferric oxide can render the entire tape useless. The form of encryption needs to match the task at hand.

It is also essential to ensure that processes are implemented within the organization that ensure that encrypted sensitive information that is sent off-site is to arrive at the location without incident (where feasible) and that it is stored correctly. It is for instance no use sending backup tapes to on-off site warehouse facility where the temperature and humidity reaches the full extent of a tropical wet season.

Lastly, the auditor needs to not only have an attestation from management stating that the encryption system is sufficiently strong, but also needs to test this assertion. This requires that the system is validated against attack and utilizes an appropriate method of encryption. The system must also be compliant with all local and international laws and regulations concerning the data and the encryption algorithms themselves.