What does it really mean when an organization says it is ISO 27001:2013 certified?

We usually come across claims by organizations that they are certified ISO 27001:2013 organization. But what does it really mean, and how does it benefit potential business partners? We will try to understand this in more details here, and explain what ISO 27001:2013 compliance means to our business partners.

Let us first understand in layman terms what ISO 27001:2013 means.

What is ISO 27001:2013?

ISO 27001:2013 is 'Information Security Management System' standard published in October 2013 by International Organization for Standardization (ISO). It specifies information management system that brings information security under explicit management control. Organizations that claim to have adopted ISO 27001 are audited and certified compliant with the standard by accredited registrars'.

Why do you need ISO 27001:2013 certification?

A lot of organizations have information security controls, which typically are implemented to address specific situations in an ad-hoc fashion. For example, security controls would be in place to address certain aspects of technology, network or digital data security. However, the organization might not have adequate security mechanisms and controls in place for traditional information assets like paper, or for physical security or business continuity planning etc.

ISO 27001 mandates creation of an over arching 'Information Security Management System (ISMS)' that creates a coherent and secure information ecosystem in the organization. Such integrated ISMS ensures that all data residing in the organization, be its own IP or its client data is available when required, to only who is privileged to access it i.e. appropriate levels of confidentiality is maintained , and in the form required without any risk of data-corruption or data loss.

What does it mean to be ISO 27001:2013 certified?

Given the above back ground, let us look at what it means when an organization claims to be an ISO 27001:2013 certified organization. It means that:

1) The organization has systematically examined its information security risks taking into account the possible threats, vulnerabilities and impact.

2) The organization has a coherent and comprehensive suite of information security controls in place to ensure confidentiality, availability and integrity of its and its client data.

3) Have an overarching management process to ensure that the information security controls are adequate to meet the information security needs & the process is reviewed on an ongoing basis.

4) The organizations information security practices are audited by independent accredited registrars for compliance to the ISO 27001:2013 standards.

How is this implemented at Mangalam?

Below are some of the key points of how data and network security is implemented at Mangalam:

- Secure FTP servers used for data transfers are audited & certified for its security.
- In-house Servers are protected using access control devices.
- Operators are not permitted to carry any removable media on to the production area. None of the workstation in production area has access to any printers. None of the workstations on the production floor have slots for removable media. We have restricted all the rights on workstations to copy or delete files. We do not permit hand baggage in the production area. We also do not allow employees to carry printed material, computer printouts or data storage media of any kind on the premises
- Every operator and Server activity is logged and monitored.
- Network is immune to any unauthorized access/hacking through active Firewall
- The main server is equipped with dual high-speed CPUs and RAID Level Five Security, ensuring failsafe redundancy
- All applications require authenticated access to the system using unique login identifier and password. We have strong password policy and all passwords contain at least 6 characters and include a combination of alphabetic and numeric characters. All the users are required to change their passwords within a specified period. By default, the password expires after 45 days and compels the users to change their password
- The system administrators designate the physical separation of data related to different applications/clients and control the access rights. This arrangement meets with general guidelines of providing access to data, strictly on a "need to know" basis. This additional layer of confidentiality helps prevent unauthorized access to client data.
- The auditing system keeps a detailed log of the user activity along with a list of all successful and failed system login attempts. Only the system administrator is authorized to run these reports to view the logged activity and only he can purge audit entries, based on a selected criterion.
- We require all employees to sign a confidentiality agreement prior to joining the company.
- We have efficient security personnel, guarding our facilities for all working shifts, seven days a week. All employees are thoroughly briefed on privacy & data security issues and they realize that any lapse on their part would normally result in termination of their employment.

About Mangalam Information Technologies Pvt. Ltd.

Mangalam is a leading offshore 'Litigation Support' Services provider, based in Ahmedabad-India. Our services cover a wide range of litigation support services including Offshore EDD Data Processing, Bibliographic Coding and Records Retrieval related services.

Our clients include some of the largest national litigation support services provider in the US, Canada, Australia and UK since more than 7 years. We are an ISO 27001:2013 certified company

For more details – Contact: sales@mangalaminfotech.com