www.isocertificationtrainingcourse.org
registrar@isocertificationtrainingcourse.org

ISO 27001 certification Steps

If your company is looking for a ISO 27001 Certification on Information Security management system (ISMS) based standard, you might be overwhelmed with figuring out where to start. To help with this, here is an overview of the steps that are needed to help you make sure that nothing is missed during your implementation and preparations for certification:

Management Support – This is most critical. Without the support of management your implementation of ISO 27001 will almost certainly fail. Plan your sales pitch well to convince your management that ISO 27001 is a good idea, and if you need some help take a look at the ISO certification Benefits Tutorial video.

Establish ISO 27001 Certification Project, Project plan and resources - Determine the cut off period by which you need to have ISO 27001 certification in place. This would enable reverse engineering of the project and importance of time lines including the early start-off date. Identify the project leader. Identify the products or services to be included in the scope of ISO 27001 certification. Do the costing. It includes implementation learning cost, and Certification fee.

Conduct ISO 27001 Awareness Training - This is required to gain A to Z of the fundamentals of ISO 27001. Need to cover all resources in the scope. This training is imparted in batches by specialist and industry expert. Evidence of training records needs to be maintained for demonstration during ISO 27001 certification audit.

Identify the ISO 27001 Implementation team- ISO 27001 implementation can no longer be tasked to single person, or group of few persons in the organization. The ISO 27001 Standard is premised on Risk Based thinking, and risk management must be done at the hands of respective departments and functions, such that head of the departments are the " Risk-Owners.

Therefore the implementation team would include Heads of the departments, deputies or other critical resources in each function, besides the central team.

Conduct ISO 27001 Implementation Training - This training is imparted by 'specialist and industry expert' to the implementation team identified by the organization. The ISO 27001 Implementation training is conducted in workshop style covering implementation practical cases of your organization and its processes. This would last upto 7 days.

Define context, scope and Policy – Defining the context, scope, and policy of your ISMS will help to ensure you know the limits of what needs to be done, so that you do not include areas of your business that might not have an effect on your system. The key tool to define the scope is the dependency matrix which will be the first document you will need to create for the ISMS.

Define RA & RT, Objectives, processes and procedures – Risk assessment and risk treatment is the backbone of ISO 27001 implementation. ISMS Objective help to conduct dipstick check of the performance levels. to Documentation will include the mandatory procedures defined by the ISO 27001 standard, but also any additional processes and procedures required by your company to ensure consistent and adequate results with respect to Information Security. The key is to define all the processes in your company and look at how they interact within your organization. It is in these interactions that problems can occur. Extent of documentation depends on size of organization, complexity of the processes and competence of the people.

Implement ISO 27001 processes and procedures – Often, these processes will already be in place at your company and will just need to be adequately documented to ensure consistent results. Not all processes need to be documented procedures, but it is important to decide which ones need to be in order to ensure compliant products and services.

Conduct ISO 27001 Internal Auditor training – ISO 27001 standard requires the organization to train team of internal auditors who would perform cross audit on another on regular basis. Internal Auditors need to be competent. To evidence the same, the organization need to a specialist Industry expert to impart ISO 27001 Internal Auditor training.

Conduct ISO 27001 internal audits – Before the Lead Auditors of certification body visits to audit your system, ISO 27001 mandates that you to audit each process internally. This will give you a chance to make sure that the processes are doing what you had planned. You will also have a chance to implement the necessary corrective actions to fix any problems that you find.

Closure activities and Corrective Action reports – This is the step where you find the root cause of any problems found during your measurements, internal audits and management review, deviations from the established processes, customer concerns and take action to correct the root cause. This is the key step toward Continual improvement, which is a main focus of having an ISO 27001 ISMS. For an explanation of the corrective action process see the tutorial on CAPA.

Conduct ISO 27001 management reviews – Just as it is important that management supports the implementation of ISO 27001, it is also important that they are fully involved in the maintenance of the ISMS. Top Management needs to review specific data from the activities of the ISMS in order to ensure that the processes have adequate resources to be effective and improve.

Pre-assessment / ISO 27001 Gap Analysis - This is done by Specialist Industry expert, to help organization in gap analysis, so that gaps identified during pre-assessment/ gap analysis are plugged before the organization

Proceeds for Certification Audit. This is very important step to raise the confidence level of the auditees.

Choose a certification body – This can be a very important step in how effective your implementation is. The certification body is the company that will ultimately come in to audit your ISMS and decide if it is compliant with ISO 27001 requirements, as well as whether it is effective and improving.

Operate & measure the ISMS – This is when you will collect the records that will be required in audits to show that your processes meet the requirements set out for them, that they are effective, and that improvements are being made in your ISMS as needed. Certification bodies need this to happen over a certain length of time (generally not less than 3 months), which they will identify, in order to ensure that the system is mature enough to show compliance.

ISO 27001 Certification audit- Stage 1 – This is a review of your documentation by the certification body auditors to verify that, on paper, you have addressed all the necessary requirements of the ISO 27001 standard. The auditors will issue a report outlining where you comply and where there are problems, and you will have a chance to implement any corrective actions to address the problems. This may take place during the timeframe defined for the initial operation of the ISMS.

ISO 27001 Certification audit- Stage 2 – This is the main audit when the certification body auditors will review the records you have accumulated by operating your ISMS processes, including your records of internal audits, management review and corrective actions. From this review, which will take several days, they will issue a report detailing their findings and whether they have found your ISMS to be effective and in compliance with the ISO 27001 requirements. The auditors will also make a recommendation for certification if you meet all requirements. If you have any major non-conformances, then you will need to take corrective action for these problems before certification can be recommended.

A good plan will help a lot when you implement ISO 27001 and work toward ISO 27001 certification, so do take the time to plan and know what resources you need – this will save you time and resources later on.

Value added ISO 27001 Certification Training & Consultancy

Accelerate learning with the expert faculty Lead Auditors and Principal Trainers from the Industry. Learning from the "Specialist Expert" has many advantages:-

- It will drastically change the way of thinking and basic approach towards the Management System Standards.
- You would cherish & Benchmark our training for a very long time to come.
- No fictitious case studies you can not connect with.
- Real time examples, real time scenarios you can quickly relate to.
- Complete Focus on your systems, processes and line of businesses.
- 100% involvement and engagement of the participants
- Learn to make the ISO Standard sweat to:-

A). Improve the profits.

B). Reduce rework, defects, customer rejections, wastage,& cost of operation

C). Enhance customer delight

D). Reduce attrition of customers and employees

E). Enhance confidence of all stakeholders