ISO 27001 Implementation Key Steps

1. Define focal person / team and their training on ISO 27001 ISMS
2. Define the scope of the ISMS – could be no of process, departments, services or product lines. Usually company include with their IT department as the starting point
3. Conducting Gap Assessment – preferably by an ISMS consultant or an ISMS auditor
4. Perform Information Security Risk Assessment (RA) to identify the threats and risks to information security. Define RA methodology with risk acceptance criteria and involve process owners
5. At this point Evaluate the 93 controls in Annex A to be implemented or any controls beyond 93 controls to mitigate the risks.
6. Controls implementation include the ISMS documentation including policies and procedures. This will develop the 'Risk treatment plan'
7. At this point, start training company workforce on information Security basics, why it is essential for the organization to comply and what will be their role
8. Training Internal Auditors and Perform Internal Audit followed by a Management Review
9. In parallel, start contacting the ISO 27001 certification body to call the external auditors to perform the certification audit
10. On successful audit, ISO 27001 certificate will be issued