**Project Checklist for ISO 27001 Implementation**

|  |  |  |
| --- | --- | --- |
| **Implementation phases** | **Tasks** | **Done** |
| *Obtain management support* | Research which benefits of ISO 27001 would be applicable to your company |  |
| Present the benefits to the management and get their commitment  |  |
| Get formal approval for the project |  |
|  |  |
| *Prepare for your project* | Decide whether you are going to use consultants or you will be using documentation templates |  |
| Purchase the ISO 27001 standard |  |
| Educate your project team |  |
| Write the project plan including the definition of project manager, project team, project sponsor, required resources and milestones |  |
| Define which stakeholders need to be informed about each step in the project |  |
| Organize kick-off meeting |  |
|  |  |
| *Identify requirements* | Identify interested parties |  |
| Identify the requirements of interested parties |  |
|  |  |
| *Define the scope, management intention and responsibilities* | Write the ISMS Scope Document |  |
| Write the Information Security Policy |  |
| Decide on the information security objectives |  |
|  |  |
| *Implement support procedures* | Write procedure for document control |  |
| Write procedure for internal audit |  |
| Write procedure for corrective action |  |
|  |  |
| *Perform risk management* | Develop the risk assessment methodology |  |
| Perform risk assessment |  |
| Perform risk treatment |  |
| Write the risk assessment & treatment report |  |
|  |  |
| *Develop security profile of your company and action plan on how to achieve it* | Develop the Statement of Applicability |  |
| Develop the Risk Treatment Plan |  |
| Accept the residual risks |  |
|  |  |
| *Implement the controls* | Implement all the controls defined in Risk Treatment Plan |  |
| Maintain records of implementation |  |
|  |  |
| *Perform training and awareness programs* | Perform training for all employees who lack required skills |  |
| Perform awareness programs for all employees and third parties that have a role in your ISMS |  |
|  |  |
| *Operate the ISMS* | Maintain all the records required by your own policies and procedures |  |
| Perform corrective actions as needed |  |
|  |  |
| *Monitor & measure the ISMS* | Make sure you monitor all your systems |  |
| Measure if you have achieved the objectives set for your ISMS and for your controls |  |
|  |  |
| *Perform internal audit* | Develop the audit program |  |
| Perform internal audit(s) |  |
| Write an internal audit report |  |
| Perform corrective actions |  |
|  |  |
| *Perform management review* | Perform management review |  |
| Maintain records from management review |  |
| Perform corrective actions |  |
|  |  |
| *Certification audit* | Obtain proposals from several certification bodies |  |
| Select the certification body |  |
| Stage 1 certification audit |  |
| Stage 2 certification audit |  |
| Surveillance visits  |  |
|  |  |