**Project Checklist for ISO 27001 Implementation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Implementation phases** | **Tasks** | **Documents from toolkit to be used** | **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 starting the project planning | - |  |
|  |  |  |
| *Prepare for your project* | Write procedure for document control | 00 – Procedure for Document and Record Control |  |
| Educate your project team | - |  |
| Write the project plan including the definition of project manager, project team, project sponsor, required resources and milestones | 01 - Project Plan |  |
| Define which stakeholders need to be informed about each step in the project | - |  |
| Organize kick-off meeting | - |  |
|  |  |  |
| *Identify requirements* | Define procedure for identifying interested parties | 02 - Procedure for Identification of Requirements |  |
| Identify the requirements of interested parties | 02.1 - List of Legal, Regulatory, Contractual and Other Requirements |  |
|  |  |  |
| *Define the scope, management intention and responsibilities* | Write the ISMS Scope Document | 03 – ISMS Scope |  |
| Write the Information Security Policy | 04 – Information Security Policy |  |
| Decide on the information security objectives | 04 – Information Security Policy |  |
|  |  |  |
| *Perform risk management* | Develop the risk assessment methodology | 05 – Risk Assessment and Risk Treatment Methodology |  |
| Perform risk assessment | 05.1 – Risk Assessment Table |  |
| Perform risk treatment | 05.2 – Risk Treatment Table |  |
| Write the risk assessment & treatment report | 05.3 – Risk Assessment and Risk Treatment Report |  |
|  |  |  |
| *Develop security profile of your company and action plan on how to achieve it* | Develop the Statement of Applicability | 06 – Statement of Applicability |  |
| Accept the residual risks | 06 – Statement of Applicability |  |
| Develop the Risk Treatment Plan | 07 – Risk Treatment Plan |  |
|  |  |  |
| *Implement the controls* | Implement all the controls defined in Risk Treatment Plan | Documents in the Folder 08 Annex A Security Controls |  |
| Maintain records of implementation | For ISMS documents this is visible through the version history of a document; for software this could be some log about its testing and release. |  |
|  |  |  |
| *Perform training and awareness programs* | Perform training for all employees who lack required skills | 09 – Training and Awareness Plan |  |
| Perform awareness programs for all employees and third parties that have a role in your ISMS | 09 – Training and Awareness Plan |  |
|  |  |  |
| *Implement management procedures* | Write procedure for internal audit | 10 – Internal Audit Procedure |  |
| Develop the audit program | 10.1 – Annual Internal Audit Program |  |
| Define which measurements are to be performed related to the objectives for the ISMS and for controls | 11.1 – Measurement Report |  |
| Identify information sources to be used in the management review | 11.2 – Management Review Minutes |  |
| Write procedure for corrective action | 12 – Procedure for Corrective Action |  |
|  |  |  |
| *Operate the ISMS* | Maintain all the records required by your own policies and procedures | Various records and logs that are created because of ISMS documents – e.g., backup log (from the backup software), filled out List of Legal, Regulatory and Contractual Requirements, etc. |  |
| Perform corrective actions as needed as a consequence of improvements needed in the operation of the ISMS | 12.1 – Corrective Action Form |  |
|  |  |  |
| *Monitor & measure the ISMS* | Make sure you monitor all your systems | Monitoring records defined in each implemented document, e.g., number of incidents, number of errors in a particular system, etc. |  |
| Measure if you have achieved the objectives set for your ISMS and for your controls | 11.1 – Measurement Report |  |
|  |  |  |
| *Perform internal audit* | Perform internal audit(s) | 10.3 – Internal Audit Checklist |  |
| Write an internal audit report | 10.2 – Internal Audit Report |  |
| Perform corrective actions as a consequence of nonconformities found during the internal audit | 12.1 – Corrective Action Form |  |
|  |  |  |
| *Perform management review* | Perform management review | - |  |
| Maintain records from management review | 11.2 – Management Review Minutes |  |
| Perform corrective actions as a consequence of improvements identified during the management review | 12.1 – Corrective Action Form |  |
|  |  |  |
| *Certification audit* | Obtain proposals from several certification bodies | - |  |
| Select the certification body | - |  |
| Stage 1 certification audit | - |  |
| Stage 2 certification audit | - |  |
| Surveillance visits | - |  |
|  |  |  |