What is Information Security Management System?

An **Information Security Management** **S**ystem (**ISMS**) describes controls that an organization needs to implement to ensure that it is sensibly protecting the **Confidentiality, Integrity & Availability** of Information from threats and vulnerabilities of respective Assets, which contain the same. ISMS includes process of Identification of Organizational Information and classify the same based on a criteria and assess the losses (in different ways) in case this information is breached (erased, stolen , removal etc.). ISMS involves the assessment of the risks an organization must deal with in the management and protection of Information as well as the dissemination of the risks to all appropriate interested parties (external or internal to the organization. As part of information security management, an organization may implement an information security management system and other best practices found in requirements of  ISO 27001:2013 & supported by guideline standards like  ISO 27002, and ISO 27035 standards on information security.



Where & how can Information Security Management System be applied?

For **Information Security Management System** (**ISMS**), be applied to any organization, irrespective of size or industry sector. ISMS principle approach has following basic principles & strategies in place:

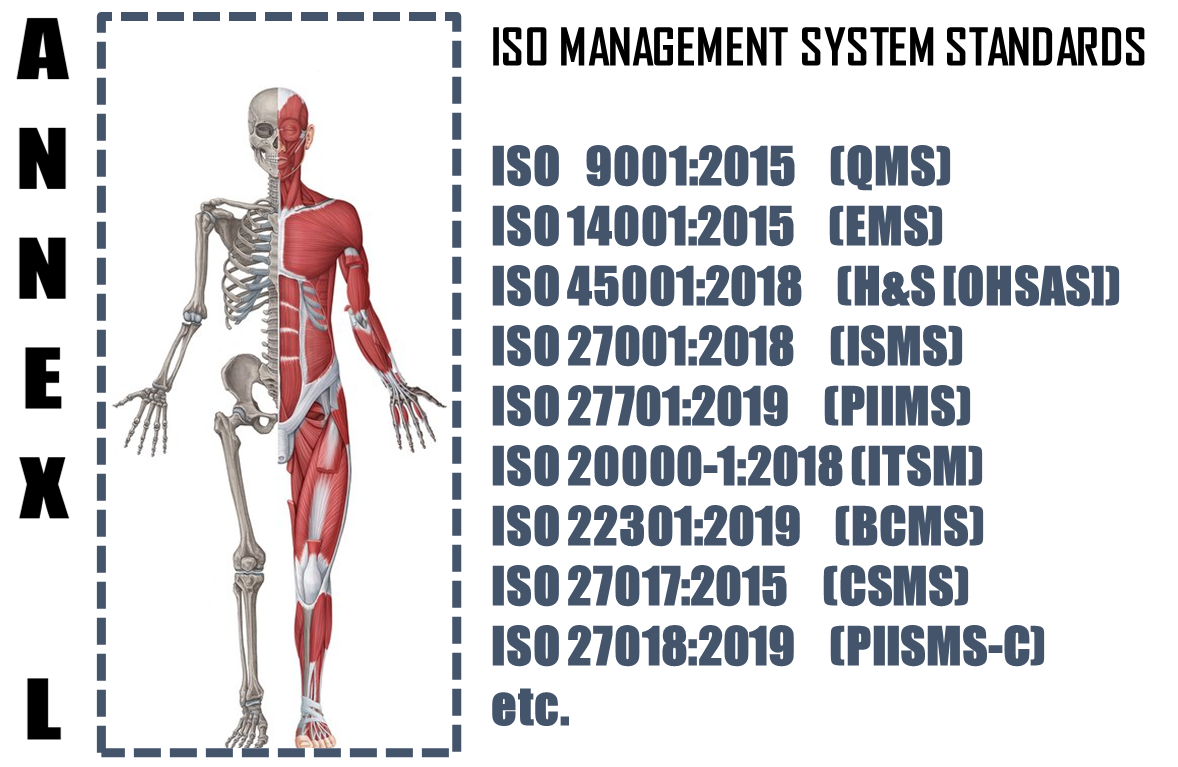
|  |  |
| --- | --- |
| Principles – QMS Principles may be considered to maintain  C, I & A of Information | Strategies |
| * Awareness for the need for ISMS      * Assignment of Responsibility for ISMS * Management Commitment for ISMS * Risk Assessment – acceptable risk * Prevention & Detection of ISMS Incident * Comprehensive Approach * Regular review & Update of ISMS | * Focus on Information Classification for the scope & context * Identify ASSETS with VULNERABILITIES for C, I & A Separately * Define Risk Assessment to identify Risk Impact of each Vulnerability on C,I & A * Perform Risk Evaluation (Impact Level) on current controls and after new controls * Use Annex A of ISO 27001:2013 to select the Vulnerability Controls for C, I & A * Understand and approve the Residual Risks & Implement the selected controls & monitor for performance |

What can make Information Security Management System journey successful?

To implement & get maximum benefited from ISMS, there has to be ***baseline mindset principles***, in which every member of the organization (including Top Management) should believe in:

|  |  |
| --- | --- |
| Mind Set for ISMS | Benefits of ISMS |
| * Clear understanding the importance of Information and its legitimate usage ! * Open mind to adopt culture for new understanding & learning concepts, technology and its vulnerabilities of the relevant Assets, in more precise manner; * Complete Transparency in understanding, implementing changes, if need be, at appropriate time; * **Always believe that, what we know today is not enough and not the end**; * Always believe in and practice team work, commitment to improve and believe in that: * **Any System to be in such a manner that people depend on System, & not the other way round**”; * Ask self-question all the time - “Am I interpreting the requirements of ISMS Standard in current manner?; * Importance has to be given to documentation with Criteria inbuilt into it for internal transparency; * **Believe in building up Process KEDB (Known Error Data Base) – and update in disciplined manner and ensure that this is accessible to every one** | * Clarity to Organization Governance to Secure Information in a better Systematic and Consistent manner; * New Risk Based mechanism shall open your minds in understanding the importance of Information, compared to time before, for future sustainability of the business; * Achieve greater consistency in the activities involved in providing security controls more effectively; * Gives opportunity to understand the limitations of security controls in the form of Residual Risks; * Increase efficiency by improving use of information in more legitimate manner. * Improve people competency in systematic manner & aim & enhance for better Information Value; * Market your business more effectively; * Exploit new market sectors and territories; * Manage growth more effectively by making it easier to integrate new employees; * Constantly improve your process compliance to regulations, on periodical basis as technology comes first and then the laws. |

What is Annexure L?



The **Annex L** (now renamed as Annex L in the 2019th edition from Annex SL) is a section of the ISO/IEC Directives part 1 that prescribes how ISO Management System Standard (MSS) standards should be written. The aim of Annex L is to enhance the consistency and alignment of MSS by providing a unifying and agreed-upon high level structure, identical core text and common terms and core definitions. The aim being that all ISO Type A MSS (and B where appropriate) are aligned and the compatibility of these standards is enhanced.

So in short we can say that Annex L is the Skeleton of ISO Management Systems and all standards are now aligned as per Annex L and all the common elements terms and definitions have also been standardized. This has been done to bring in Standard in the Structure, which was not the case in the past, though the intention was the same. So we can say, out of Intent and Content of MS, Content has undergone a change, in the form of Anne L.

What to do in Implementing Information Security Management System?

Based on the Scope and Context, following activities have to be performed in logical sequence. These guidelines given below are only basic milestones and a lot of activities may have to be streamlined as per the standard, based on Scope & Context.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step #** | **Requirement of ISMS** | **What needs to be done (**C, I & A Separately) | **In what way IRCBO can contribute** | **Tools Recommended** |
| 1 | Defining & Documentation | * Defining & Documenting Scope (Technical [Product/Services] and Territorial Scope (# Locations) where the MS is needed. The Org. Management decides the specific scope in line with Applicable regulations * Defining the External & Interested Parties, their business relationship with Org. (in relevance to scope), Identification of critical processes, Information & Information classification); * All relevant policies and procedures for delivery of products and services, as per scope & context - these procedures or process documents for each interested party activities shall include acceptance criteria as well – including Design of Product/Service Processes; | IRCBO’s Qualified & Experienced consultants can help you in designing, defining, Implementing, monitoring and Improving the MS.  Note: Our contracts can also be associated after Certification for Maintenance of Management System through our digitized tool contributions – aim is to make any MS a plug and play for most effective Controls & Complying (including Legal Compliances) | IRCBO Tool Kit which includes all solutions for Implementation and backed up by IRCBO Designed Software in cloud for :   * Online training   (including  Induction for new employees, awareness & unlimited Internal Auditor Training & Qualification   * Online Internal Auditing Software – this also includes tracking of corrective actions |
| 2 | Implementation | * Implementing all policies and procedures as per ISMS defined system; * Assigning and plying Responsibilities and Authorities in more transparent manner; * Participating in Risk Mechanism and approving Residual Risk and Incident investigations – for C, I & A Separately * Focusing on Increasing Competency, * Maintaining good discipline in demonstrating Leadership and aiming for improvements through Management Review platforms; |
| 3 | Periodical Review | * Monitoring, measuring and performing Analysis to ensure * Considering Internal Audit Findings seriously for Timely Corrective Actions in effective manner and take decisions to improve in Management Reviews |
| 4 | Continual Improvement | Implement all actions of Management Review and aim for Continual Improvement – remember Improvement & Continual Improvement are different Concepts |