What is IT Governance Management System?

**ISO 38500** is an international standard for Corporate governance of information technology published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations’ use of IT.

**BUSINESS PERFORMANCE IT GOVERNANCE**



management system.

ISO/IEC 38500:2015 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization.

ISO/IEC 38500:2015 defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.

Where & how can IT Governance Management System be applied?

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

|  |  |
| --- | --- |
| Principles – IT-GMS Principles may be considered to maintain C, I & A of Information | Strategies |
| * Understanding Scope & Context to

* Source of IT-GMS Understanding
* Management Commitment for

 IT-GMS * Risk Assessment

– all Interested Parties in IT-GMS* Prevention & Detection of IT-GMS

 Incident* Comprehensive Approach
* Regular review & Update of IT-GMS
 | * Focus on Source of IT-GMS in the Scope & Context of products & services
* Identify VULNERABILITIES of IT attracting IT-GMS

(Average Risk Appetite of Human Population – life style)* Define Risk Assessment to identify Risk Impact of each Vulnerability of IT-GMS
* Perform Risk Evaluation (Impact Level) on current controls and after new controls of IT-GMS
* Ensure that approval process by different basis to be strengthened (with criteria) which is one of the best method – easy to implement – where ever More or Strong Vulnerabilities
 |

What can make IT Governance Management System journey successful?

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

|  |  |
| --- | --- |
| Mind Set for IT-GMS  | Benefits of IT-GMS  |
| * Clear understanding the importance of IT-GMS and its impacts on businesses and society;
* Open mind to adopt culture for new understanding & learning concepts, technology and its vulnerabilities of the IT-GMS opportunities, in more precise manner;
* Complete Governance Supporting IT Governance in meeting Business Goals;
* **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 IT-GMS can be controlled;
* **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 IT-GMS Standard in correct 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;
* An alignment between Corporate Governance & IT Governance in ensuring the Interested party’s business Goals are maximum IT driven to reduce the people dependency;
* 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;
* 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 IT Governance 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 IT-GMS**  | **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 -IT-GMS 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 IT-GMS 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 |