SELF EVALUATION CHECKLIST

ISO/IEC 27001:2022

*Designed by Ranasinghe R.A.D.T.M*

*IT22560094*

This document is intended to assist you in the identifying your readiness for becoming 3rd party certified to the globally recognized standard ISO/IEC 27001:2022 Information Security Management System (ISMS). When the checklist has been completed, you may contact us to organize a GAP assessment or get started on your Certification Audit.

|  |  |
| --- | --- |
| **Company Name:** |  |
| **Proposed Scope of Certification:** |  |
| **Completed by:** |  |

**Before you begin with give thought to...**

# Policy and Leadership

* Do we have a clear and docmen ed Information Security Policy that defines our commitment to protecting our information assets?
* Is our senior management committed to Information Security and actively involved in promoting and supporting the implementation of an ISMS?
* Do we have a designated Information Security Officer or team responsible for managing and implementing the ISMS?

# Risk Assessment

* Have we conducted a risk assessment to identify the risks and threats to our information assets?
* Have we identified the impact of potential information security incidents on our business operations and reputation?
* Have we identified the risk owners and their responsibilities for managing risks?
* Do we have a risk treatment plan that outlines the measures to be taken to mitigate identified risks?

# ISMS Implementation

* Have we identified the information assets that we need to protect?
* Have we established information security objectives and defined metrics to measure their effectiveness?
* Have we defined roles and responsibilities for all personnel involved in the ISMS implementation?
* Have we established procedures for incident management and reporting?
* Have we established access controls and defined procedures for granting and revoking access to information assets?
* Have we established procedures for managing third-party service providers and their access to our information assets?
* Have we established procedures for managing the physical security of our information assets, including the protection of devices and media containing sensitive information?
* Have we implemented procedures for monitoring and detecting security incidents and breaches?
* Have we established procedures for managing and reporting security incidents and breaches?

# ISMS Maintenance

* Do we regularly review and update our Information Security Policy, risk assessments, and risk treatment plan?
* Do we conduct regular internal audits of our ISMS to ensure compliance with ISO 27001 and our own policies and procedures?
* Do we conduct regular management reviews of the ISMS to ensure its effectiveness and suitability for our organization?
* Do we continually improve our ISMS by identifying areas for improvement and implementing corrective actions?

# Training and Awareness

* Do we provide regular training and awareness programs to all employees on Information Security policies, procedures, and best practices?
* Do we provide specific training and awareness programs for personnel with access to sensitive information assets?

**CHECKLIST ISO/IEC 27001:2022**

Next follows the requirements of the standard. You may use the last column to insert your management system documentation reference.

**Context of the organization**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 4.1  Understanding the organization and its context | * External issues have been determined. * Internal issues have been determined. |  |
| 4.2  Understanding the needs and expectations of interested parties | * Interested parties relevant to the ISMS identified * All relevant information security requirements of these interested parties identified |  |
| 4.3 The organization shall determine the boundaries and applicability of the information security management system to establish its scope. | * The internal and external issues * Interested parties needs and expectations * Organization of activities performed * Services * Third party services * Location * Exclusions from scope have been justified |  |
| 4.4 The organization shall establish, implement, maintain and continually improve an ISMS, including the processes and their interactions | * The necessary processes and their interactions are included |  |

**Leadership**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 5.1 Top management shall demonstrate leadership and commitment with respect to the ISMS | * Management provides formal support for the implementation and operation of the ISMS * IS policy and the IS objectives are established * Integration of the ISMS requirements into processes * Communication regarding the ISMS and of conforming to its requirements * Resources are available |  |
| 5.2 ISMS Policy | * Is appropriate & includes objectives * Includes commitment to requirements * Includes commitment to continual improvement * Is documented * Is communicated * available |  |
| 5.3 Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization | * Ensuring that the ISMS conforms to the requirements of the standard * Reporting on the performance of the ISMS to top management |  |

**Planning**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 6.1 Actions to address risks and opportunities | **Our organization has planned.**   * The actions necessary to address documented risk and opportunities related to the implementation of the ISMS * How to integrate and implement these actions into the ISMS * How to evaluate these actions   **Risk Assessment**   * Is defined and documented * Includes business IS requirements * Includes legal and statutory requirements * Includes criteria for risk acceptance and acceptable levels of risk * Identifies organizations risks and risk owner * Identifies impacts on confidentiality, integrity, and availability * Risks are analyzed and evaluated * Realistic likelihood of IS failures have been studied * Risks have been accepted or mitigated as per defined methodology   **Risk Treatment**   * Is defined and documented * Risk treatment options are selected * Controls are determined * Includes controls from Annex A and a verification that no necessary controls are omitted.   **Statement of Applicability**   * Is defined and documented * Contains controls and justification of inclusion and exclusion of these * Contains status of selected controls * Contains a formulated risk treatment plan, risk owner and the owner’s approval of risk treatment plan and acceptance of residual risk |  |
| 6.2 The organization shall establish IS objectives at relevant functions and levels | **Objectives are.**   * Consistent with IS Policy * Measurable * Taking IS requirements and results from risk assessment/ treatment into account * Monitored * Communicated * Documented * Planned to be achieved |  |
| 6.3 Planning of changes. | * When need for changes to the ISMS, the changes are carried out in a planned manner |  |

**Support**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 7.1 Resources | * Resources needed for establishment, implementation, maintenance and continual improvement are determined and provided |  |
| 7.2 Competence | * Competency requirements are determined * Management ensures that the competency of persons in scope is appropriate * Documented information as evidence of competence is retained * A training & awareness program is developed |  |
| 7.3 Awareness | **Persons in scope are aware of**   * The IS Policy * Their contribution to the ISMS * The implications of not conforming with the ISMS |  |
| 7.4 Communication | * The need for internal/external communication has been determined |  |
| 7.5 Documented information | **Documented information**   * Has identification and description * Is formally approved * Is available and protected * Is subject to version and change control, review and re-approval |  |

**Operation**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 8.1 The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6 | * Documented information is available to the extent necessary to have confidence that the processes have been carried out as planned * Planned changes are controlled and consequences of unintended changes is reviewed * Externally provided processes, products or services that are relevant to ISMS is controlled. |  |
| 8.2 IS risk assessment | * Risk assessment is performed at planned intervals * Risk assessment is performed when there are significant changes * Is documented |  |
| 8.3 IS risk treatment | * Risk treatment plan is implemented * Results are documented |  |

**Performance Evaluation**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 9.1 Monitoring, measurement, analysis and evaluation | * Process is established * Evidence of results is documented * Performance and effectiveness of the ISMS is evaluated |  |
| 9.2 Internal audit | * Is conducted at planned intervals * Internal audit programmed is established * Evidence of results is documented |  |
| 9.3 Management review | * Results of management review include decisions related to continual improvement * Results of management review includes needs for changes to the ISMS * Is documented |  |

**Improvement**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| 10.2 Nonconformity and corrective action | * NCs are actioned and corrected * Potential causes to NC’s are identified and eliminated * Effectiveness of CA’s are evaluated * Are documented |  |

**Mandatory documents & records**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Your organization** | **Document reference** |
| According to ISO 27001, the documented information specified in the next column is required to be produced | * Scope of the ISMS (clause 4.3) * IS Policy (5.2) * IS Risk Assessment and Treatment process (6.1.2) * Statement of Applicability (6.1.3) * IS Objectives (6.2) * Risk Assessment and Treatment report (8.2 and 8.3) * Inventory of assets (A.5.9\*) * Acceptable use of assets (A.5.10\*) * Incident response procedure (A.5.26\*) * Statutory, regulatory, and contractual requirements (A.5.31\*) * Security operating procedures for IT management (A.5.37\*) * Definition of security roles and responsibilities (A.6.2 and A.6.6\*) * Definition of security configurations (A.8.9\*) * Secure system engineering principles (A.8.27\*) |  |
| ISO 27001 records that are mandatory | * Trainings, skills, experience, and qualifications (Clause 7.2) * Monitoring and measurement results (9.1) * Internal audit program (9.2) * Results of internal audits (9.2) * Results of the management review (9.3) * Results of corrective actions (10.2) * Logs of user activities, exceptions, and security events (A.8.15\*) |  |