

Contents

[1. ISO 27001 IMPLEMENTATION SCOPE: 2](#_Toc121818993)

[2. Project Deliverables 3](#_Toc121818994)

[Responsibilities 4](#_Toc121818995)

[INFOCUS-IT Responsibilities 4](#_Toc121818996)

[CLINET ‘*s* Responsibilities 4](#_Toc121818997)

[3. ISO27001 PROJECT DELIVERABLES 8](#_Toc121818998)

[4. Time Frame 10](#_Toc121818999)

[Phase I - Project Initiation 10](#_Toc121819000)

[Phase II – Implementation 10](#_Toc121819001)

[Phase III – Implementation 11](#_Toc121819002)

[5. METHODOLOGY FOR COMPLETION OF PROJECT 11](#_Toc121819003)

[6. MAINTENANCE: 11](#_Toc121819004)

# ISO 27001 IMPLEMENTATION SCOPE:

The ISO 27001:2022 consultancy services will cover the following activities:

1. Review Information Security policies, processes and procedures of all Teams which are relevant to managing risk and improving information security to deliver results in accordance with <CLINET NAME>strategic needs and objectives
2. Perform a gap analysis on current compliance in order to assess and evaluate the controls to be implemented to achieve ISO 27001:2022 certification and accreditation.
3. Provide assistance to <Clinet Name>internal team for closure of identified gaps.
4. Review, revise or formulate documents to address ISO 27001:2022 standard requirements. The required documentation will also include the steps to be performed for ongoing compliance.
5. Revise and improve risk assessment & treatment methodology to address ISO 27001 requirements.
6. Conduct detailed risk assessment across all functions and processes under the scope and develop / updated risk mitigation & treatment plans.
7. Prepare a detailed risk report for all Functions.
8. Prepare a risk management presentation, highlighting the major findings and recommendations.
9. Implement an Information Security Management System based on the requirements of ISO27001:2022.
10. Technical review of security of information systems based on parameters identified by <CLINET NAME>and as an outcome of the gap analysis.
11. Define Key Performance Indicators(KPIs) and metrics aligned with <Clinet Name>Information security objectives driven by strategic objectives.
12. Perform an internal audit post closures of gaps to assess implementation level of ISO 27001:2022 Standard.
    1. **ISO27001 Awareness Campaign to Key Stake holders**

INFOCUS-IT will support key stake holder engagement during this consulting project. ISO 27001:2022 awareness sessions will be imparted to stakeholders and these sessions shall be tailored to meet stakeholder needs and expectations from ISMS.

# Project Deliverables

* 1. **ISMS Scoping Document**

Upon the management decision taken on the scope the ISMS Scoping Document will be produced including key business processes, personnel, information assets, information technology systems infrastructure, physical sites, external third parties/interfaces and Services provided to <CLINET NAME>’s subsidiaries.

* 1. **Assets Modeling, Identification, Information Security Valuation &Classification**

Revise current Asset Identification and Valuation for <CLINET NAME>divisions and suggest improvements and identify gaps in Asset Modeling, Identification, Classification and Information security Valuation of assets.

* 1. **Risk Management - Risk Assessment & Risk Mitigation**
     + **Threat Assessment:** Formulate Information Security threat profile for identified assets
     + **Risk Assessment & Treatment Plan & Report:** As mentioned in section
  2. **Review, Enhance or Develop Information Security Policies, Procedures & other documents for teams as required by the ISO 27001:2022 standard.**
  3. **Revise, align and update all existing documentation for applicable standards and regulations such as ISO27001.**

## Responsibilities

## INFOCUS-IT Responsibilities

1. Protect the confidentiality of <CLINET NAME>information and documentation.
2. Maintain the project delivery according to an approved Project Plan.
3. Provide regular project progress updates against approved timeframes and notify the Project Sponsor at the earliest, of any action or problem foreseen that may jeopardize the successful completion of the project or the performance of the Project Team.
4. Perform their services in a professional manner and work closely with the Project Sponsor and <CLINET NAME>representatives.
5. Ensure all outstanding problems associated with the project are resolved to <CLINET NAME>’s satisfaction.

## CLINET ‘*s* Responsibilities

1. Provide a SPOC ( Single point of contact) for smooth delivery of project.
2. Provide the overall direction and decision making for the project.
3. Provide <CLINET NAME>authorizations as necessary.
4. Provide timely access to appropriate personnel.
5. Provide details of <CLINET NAME>business and policies and guidance.
6. Project acceptance and signoff.

| **ISO 27001 IMPLEMENTATION RESPONSIBILITIES:** | | | | |
| --- | --- | --- | --- | --- |
| **Task No.** | **Task** | **Task**  **Description** | **<CLINET NAME>**  **Responsibilities** | **INFOCUS-IT**  **Responsibilities** |
| 1 | Initial Phase | 1. Conduct project kick-off meeting. 2. Definition of ISMS scope and boundaries. 3. Set up Project Steering Committee. | 1. Coordinate with Team members for their participation 2. Providing the overview of the Organization structure. 3. Allocation of Roles, responsibilities & Authorities to the Team members in ISMS Steering committee to drive the ISMS Process. | 1. Conducting Kick Off meeting explaining the need and expectations from the team members. 2. Creating the required documents defining the scope and Boundaries 3. Creating ISMS Organization Chart in line with ISO 27001 Requirements. |
| 2 | Planning Phase | 1. Establish Project time-frames. 2. Submit final project plan to <CLINET NAME> 3. Discussion and agreement on the approach methodology, audit tools and reporting. 4. Gathering of required system information, process details and organize project plan. 5. Finalize project management plan. 6. Introductory workshop for key champions and stakeholders Design of ISMS Charter (Key stakeholders, roles and responsibilities, etc.). | 1. Allocating the Project Manager and team members from different teams to ensure on-time deliverables of the Project. 2. Ensuring the availability of required team members as per the project plan requirement. 3. Providing the required technical information for the project planning. 4. Providing the proposed target dates for completion of tasks. | 1. Compile Project Plan in consent with <CLINET NAME>Team schedule. 2. Allocation of required resources for defined tasks of the project plan |
| 3 | Gap Analysis | 1. Review of critical applications, systems and network, architecture. 2. Review of access controls. 3. Review of existing information security policies. 4. Conduct interview with key champions. 5. Prepare Gap Analysis report with respect to ISO/IEC 27001:2022. 6. Submit Gap Analysis report for <CLINET NAME>Approval. | 1. Availability of team members to be a part of the Gap Analysis Audit. 2. Availability of required accesses and artifacts to conduct the audit. 3. Availability of required policy and procedure documents to conduct the review. | 1. Availability of resource to conduct the audit. 2. Prepare Gap Analysis report as per ISO 27001 standard requirements. |
| 4 | Asset management | 1. Review of existing information assets inventory and Guidelines. 2. Design of Information asset management framework in accordance with ISO 27001 requirements. 3. Finalize Information Asset Registers for processes within ISMS scope. 4. Approval of Information Asset Register. | 1. Availability of team members to be a part of the Asset Inventory guidelines. 2. Availability of required policy and procedure documents to conduct the review of Asset Inventory Guidelines. 3. Getting the required approvals | 1. Review of Asset Inventory Guidelines. 2. Designing of Information asset management framework in accordance with ISO 27001 requirements. |
| 5 | Risk Management | 1. Review existing risk assessment methodologies. 2. Review criteria for risk treatment and acceptance. 3. Development of final risk assessment framework suited for <CLINET NAME>’s ISMS. 4. Approval of risk assessment methodology. 5. Identify and evaluate options for risk Treatment Plan. 6. Select control objectives and controls for the treatment of risks. 7. Develop Risk Treatment Plan (explaining how risks will be mitigated, transferred and accepted). 8. Prepare detailed Risk Report for <CLINET NAME>’s Steering Committee approval. 9. Prepare Risk Management presentation highlighting critical findings and recommendations. | 1. Availability of team members to be a part of the Risk Assessment Review. 2. Availability of required policy and procedure documents to conduct the review of Risk Assessment Methodology. 3. Getting the required approvals | 1. Review of Risk Assessment Guidelines. 2. Designing of Risk management framework specifying Risk Assessment & Risk Treatment in accordance with ISO 27001 requirements. 3. Prepare Risk Management presentation highlighting critical findings and recommendations. |
| **6** | **Statement of Applicability** | 1. The control objectives, controls and the reasons for their selection based on identified risks. 2. The control objectives and controls currently implemented. 3. The exclusion of any control objectives and control and the justification for their exclusion. 4. Submit Statement of Applicability for <CLINET NAME>approval. | 1. Availability of team members to be a part of SOA formation. 2. Getting the required approvals | 1. Compiling SOA and Submitting it to the <CLINET NAME>Management**.** |
| **7** | **Develop, Review and align existing**  **Policies, Procedures** | 1. Review and enhance existing policies and procedures for ISMS. 2. Develop additional policies, procedures and guidelines 3. Submit all Security Policies, Procedures and Guidelines for <CLINET NAME>approval. 4. Review of existing BCP related documentation with respect to ISO 27001 requirements. 5. Create applicable document addressing the requirements Approval by <CLINET NAME>. | 1. Availability of policies and procedures for the review. 2. Availability of resources to provide inputs during the review of Policies. 3. Availability of Business Continuity Team for review. 4. Getting the required approvals | 1. Review and enhance existing policies and procedures for ISMS. 2. Develop additional policies, procedures and guidelines and Submit all Security Policies, Procedures and Guidelines for <CLINET NAME>approval. 3. Create applicable document addressing the requirements Approval by <CLINET NAME>. |
| **8** | **Trainings** | 1. Organize Information security trainings as identified. 2. Submit training attendance report for <CLINET NAME>approval. | 1. Ensure the availability of identified team members for training. | 1. Conducting the training. 2. Submit training attendance report for <CLINET NAME>approval. |

# ISO27001 PROJECT DELIVERABLES

| **Task** | **Deliverables** |
| --- | --- |
| **1. Gap Analysis** | **Deliverables** |
| Kick Off Meeting  &  GAP Analysis | 1. Kick-Off Meeting  2. Understanding the Organisation |
| 3. ISO27k Gap Analysis 4. Preparation of GAP Analysis |
| **2.Document Preparation** | **Deliverables** |
| Preparing  Policies, Processes, Guidelines  &  Checklists | 1. SOA |
| 2. ISMS Manual |
| 3.ISMS Reports for All Verticals& Implementation of ISMS Compliance Procedures to Monitor the ISMS |
| 4. Performing Risk Assessment & Updating Registers |
| 5. Creating and Updating Asset Registers |
| 6. ISMS Matrices |
| 7. Standard Operating Procedures |
| 8. ISMS Policy Statement. |
| 9. Incident Reports |
| 10. Audit Reports for all Verticals |
| 11. CAPA Templates |
| 12. BCP Methodology and Test Report |
| 14. ISMS Performance Analysis Reports |
| **3. Implementation & Trainings** | **Deliverables** |
| Preparing Onsite Training Material | 1.Basic Overview of ISMS  2.Audit Checklists for Diff Teams |
| Training the Teams | Training the Teams on ISO 27001 Requirements & Internal Auditor Training for successful implementation |
| Policies & Guidelines | Sharing the Process docs and relevant trackers to all Teams for Implementation |
| Updating the Trackers & Getting all Docs Ready | Updating the Trackers & Getting all Docs Ready |
| Follow ups for Closing the GAPs | Implementation of controls and closure of Gaps. |
| **4. Internal Audit Plan** | **Deliverables** |
| Management Team Audit | Conducting Audit & Sharing the Shortcomings with Teams |
| Admin Team Audit | Conducting Audit & Sharing the Shortcomings with Teams |
| HR Team Audit | Conducting Audit & Sharing the Shortcomings with Teams |
| IT Team Audit | Conducting Audit & Sharing the Shortcomings and Training the Teams |
| Operations Team Audit | Conducting Audit & Sharing the Shortcomings and Training the Teams |
| Legal Team Audit | Conducting Audit & Sharing the Shortcomings with Teams |
| Finance Team | Conducting Audit & Sharing the Shortcomings and Training the Teams |
| ISMS Team | Conducting Audit & Sharing the Shortcomings and Training the Teams |
| **5. Review of Implementations** | **Deliverables** |
| Management Review Meeting | Review of open Gaps along with Management and compiling the plan for closure. |
| Review of Audit Results and Prepare ness for Initial Visit of Certification Body | Review of Internal Audits. Discussions on closure actions for Initial Visit by CB |
| **6. Project Closure** | **Deliverables** |
| Closure of Final Gaps | Implementation of controls and closure of final Gaps. |
| Closure Meeting | Sharing the Final report with Management. ISMS team to continue working on implementation of Standards. Closure of ISO 27001 Certification Project. |

# Time Frame

The estimated time shall be 4-6 weeks , after the award of work order contract, however the same can be curtailed depending upon the commitment of Client’s Project team. The exact Road Map for the implementation will be prepared during first visit to Site after review of existing System and one to one discussion with client’s Project team.

| **Phase/Activities** | **W1** | **W2** | **W3** | **W4** | **W5** | **W6** |
| --- | --- | --- | --- | --- | --- | --- |
| **Phase I - Project Initiation** |  |  |  |  |  |  |
| **Project Scope Definition & Finalization** | X |  |  |  |  |  |
| **Setting project goals and objectives** | X |  |  |  |  |  |
| **Forming Core Team and appointment of Management Representative** | X |  |  |  |  |  |
| **Orientation Training on ISO 270001 to key stakeholders** | X |  |  |  |  |  |
| **Roles and Responsibilities for ISMS** |  | X |  |  |  |  |
| **Review of document Inventory** |  | X |  |  |  |  |
| **GAP Analysis w.r.t requirement s of ISO 270001 for establishing a Information Security Management System** |  | x |  |  |  |  |
| **Phase II – Implementation** |  |  |  |  |  |  |
| **Help the organization establish Objectives, Policies and plan** |  | x | x | x | x |  |
| **Help the organization is establishing asset management process and Risk Assessment** |  | X | X | x | x |  |
| **Documentation of Process & Policies for ISMS; and Common procedure** |  | X | X | x | x |  |
| **Guide the Organization in establishing a system for KPI based Monitoring for ISMS** |  | X | X | x | x |  |
| **Process Validation** |  |  | x |  |  |  |
| **Phase III – Implementation** |  |  |  |  |  |  |
| **Rollout Plan** |  |  | X | x | x |  |
| **Training of Internal Team (by Client)** |  |  | X | x | x |  |
| **Rollout Review (Off-Line)** |  |  | X |  |  |  |

# METHODOLOGY FOR COMPLETION OF PROJECT

* Signing of the agreement & NDAs by both of the parties
* Preparation of Descriptive & Detailed Plan.
* Conducting required activities as per project plan.
* Preparing Reports.
* Getting Corrective and Preventive Actions
* Getting the organization certified for ISO 27001

# MAINTENANCE:

Once ISO 27001 closures are implemented, the organization will be required to undergo periodic maintenance and Audits to ensure that the system is being maintained. The intention is to provide feedback on system performance. **The cost of maintenance can be discussed separately**.