

Presented TO: <<Client Name>>

SECUREYES

US | India | UAE | Oman | KSA

Version 1.0

November 16, 2018

ISO 27001 Current State Understanding

# Introduction

SecurEyes thanks you for giving us this opportunity to provide our specialized ISMS consulting services. As the first step in the consulting we gather a detailed understanding of the current state of ISMS within the Organization & its business objectives. The below list of questions will also help us to understand the features, functions and design of the ISMS and assist us to gauge the time and effort needed to perform the Information Security Management System gap analysis and enhancement.

# General Queries

1. Details of the organization highlighting the nature of business

|  |  |
| --- | --- |
| Nature of business |  |
| Locations of Business |  |
| Primary Driver for ISMS (regulation, statutory need, security risks, anything else) |  |

1. Is the organization for first time initiating a security or risk assessment program? If No, please list the past security initiatives chronologically?

(Yes or NO)

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. |  | Date | Past Security Initiative(s) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Has the organization been certified with any ISO standards? If yes, please list them. Please list down all the departments and locations that are within the scope of ISO?

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | ISO Specification | Year of Certification | Department/Services /Locations Certified |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. What is the scope of the proposed ISO (e.g. the business area/department/function) that needs to be ISO 27001 certification?
2. How many locations & departments are present in the scope?
3. How many employees are present in the organization? Please provide department-wise breakup.
4. How many business applications (web & thick client) are to be included in the scope? Also provide how many login modules, application roles, number of application pages are present in each application.
5. Is there an Information Security practice / department?
6. How many people are present in the department?
7. What is the total strength of the IT team?
8. Is there any inhouse development team?

# Policy Documentation

Please state whether the organization has formulated any of the following Policies? What are the various organizational documents available pertaining to Information security? (Management level and technical level policies, procedures, management intent…)

Please mention Y or N where ever applicable in the column ‘Yes’ or ‘No’ respectively

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Policies | Yes | No |
|  | Information Security Policy |  |  |
|  | IT Policy |  |  |
|  | Business Continuity Policy |  |  |
|  | Acceptable Use Policy |  |  |
|  | Personnel Security / HR Policy |  |  |
|  | Access Control Policy |  |  |
|  | Asset classification and Control |  |  |
|  | Operations and Communications Security |  |  |
|  | Physical and Environmental Security |  |  |
|  | Application Lifecycle Policy |  |  |
|  | Business Continuity Planning Documents |  |  |
|  | Compliance Policy |  |  |
|  | IT and Cyber Security Roles & Responsibilities |  |  |
|  | Information Security Incident Management |  |  |
|  | Cryptography / Encryption Policy |  |  |
|  | Vulnerability Management Policy |  |  |
|  | IT Operations Procedures, SOP’s, Processes |  |  |
|  | Network Security Policy |  |  |
|  | *<<Additional Policies & Procedures>>* |  |  |
|  |  |  |  |
|  |  |  |  |

# In-house Infrastructure Information

Following table lists the infrastructure details. Please append further detail or systems, if required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Device Type | Make  (Cisco, Juniper etc.) | Version | No. of Systems |
|  | Routers |  |  |  |
|  | Switches |  |  |  |
|  | Firewalls |  |  |  |
|  | WAF |  |  |  |
|  | IPS/IDS |  |  |  |
|  | TPAM |  |  |  |
|  | WAF |  |  |  |
|  |  |  |  |  |
|  | *<<Additional Devices/Systems>>* |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | System Type | System version  (IIS 7.0, MSExchange 2017 etc.) | Base O.S.  (Windows Server 2012, Red Had | No. of Systems |
|  | Web Servers (IIS, Apache etc.) |  |  |  |
|  | App Servers (IIS, Websphere etc.) |  |  |  |
|  | DB Servers (MSSQL, Oracle etc.) |  |  |  |
|  | Active Directory |  |  |  |
|  | Exchange Server |  |  |  |
|  |  |  |  |  |
|  | *<<Additional Devices/Systems>>* |  |  |  |

# Cloud Infrastructure Information

Following table lists the infrastructure details on the cloud. Please append further detail or systems, if required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Device Type | Make  (Cisco, Juniper etc.) | Version | No. of Systems |
|  | DDoS Solution |  |  |  |
|  | APT Solution |  |  |  |
|  | WAF |  |  |  |
|  |  |  |  |  |
|  | *<<Additional Devices/Systems>>* |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | System Type | System version  (IIS 7.0, MSExchange 2017 etc.) | Base O.S.  (Windows Server 2012, Red Had | No. of Systems |
|  | Web Servers (IIS, Apache etc.) |  |  |  |
|  | App Servers (IIS, Websphere etc.) |  |  |  |
|  | DB Servers (MSSQL, Oracle etc.) |  |  |  |
|  | Active Directory |  |  |  |
|  | Exchange Server |  |  |  |
|  |  |  |  |  |
|  | *<<Additional Devices/Systems>>* |  |  |  |

# Application Details

Please provide the following details for each application.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Application Name | Short Description | Is this an internet facing application or internal application | Is this a Web based or Thick Client Application | Is this developed Inhouse /Vendor /Outsourced/Cloud Service | No. of User Roles | Approx. No. of dynamic pages |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Hardening / Minimum Baseline Security

Are any hardening or minimum baseline security document drafted for any of the system. If yes, please mention the systems for which hardening documents are present? (Y or N)