



Q4A MANAGEMENT FZE LLC
Request for Proposal cum Application Form
Standard Multi-System Certification Audit Application

AUD-F-02
Rev.: 05

Name of Organization								
Address								
Additional Sites / Addresses, If any	NA							
Contact Numbers				Email Id				
Contact Person				Designation				
Mode of Working (i.e Online/Onsite/Hybrid)	☐ Online ☐ Onsite ☐ Hybrid (Online + Onsite)			Incase of Hybrid, Core activities Online or Onsite				
Mode Of Audit	☐ Onsite Audit ☐ Remote Audit (ICT) ☐ Blended (Hybrid)							
Scope of Certification								
Main Processes / Activities				Outsourced Processes, if any				
Standard(s)								
	☐ ISO 9001:2015	☐ ISO 14001:2015	☐ ISO 45001:2018	☐ ISO 22000:2018	☐ ISO 27001:2022	☐ ISO/IEC 27701:2025		
					☐ Others: _____			
	☐ ISO/IEC 42001:2023	☐ ISO 22301:2019	☐ ISO 37001:2016	☐ ISO 21001:2018				
Application Type	☒ Initial Certification ☐ Surveillance ☐ Recertification ☐ Scope Extension ☐ Transfer							
No. of Employees	Total				Contractual	0	Working No. of Shifts	1
Activities	Full Time	Part time	Performing Same type of Job	Temporary Unskilled workers	Effective No. of Employees, Filled by Q4A			
Management	0	0	0	0	0			
Quality / Safety / Technical	0	0	0	0	0			
Administration / HR / Accounts	0	0	0	0	0			
Maintenance / Engineering Support	0	0	0	0	0			
Ground Support / Dispatch / Other	0	0	0	0	0			
No. of personnel working away from site?(If applicable)	0	0	0	0	0			
No. of Employees	0	0	0	0	0			

MANAGEMENT SYSTEM INFORMATION(S)

1. Applicable Legal, statutory & regulatory act: (i.e., Labour law)	
2. Organization Key Process Area: (i.e., purchase/store/production etc.)	
3. Organization Products/Services: (i.e., abc & xyz products etc.)	
4. Any outsourcing process: (i.e., printing etc.)	
5. Consultant details, if used for Management System Preparation:	NA
6. Management System establishment / revision date:	

7. Manual Date			
8. Internal audit date (Or planned date):			
9. Management review date (Or planned date):			
Certified standards:		Certification Body	
Issue Date:		Expiry Date:	
ISO 14001:2015 / ISO 45001:2018 – ADDITIONAL DETAILS (FILL OUT APPLICABLE DETAILS)			
Select Condition of your location, If non of below then specify here:			
Special countermeasure area		Protection area of source water	Industrial complex
			City
Operating air emission facility: ☐ YES ☐ NO		Operating waste water treatment facility? ☐ YES ☐ NO	
Kind of wastes & amount (Ton/year):		Usage of hazardous chemical substances ? ☐ YES ☐ NO	
Does you have Pollution Clearance from local authorities? ☐ YES ☐ NO			
Does you have more than 5 critical environmental aspect or OHSAS risks? (ex: air, water, waste, noise, chemical, soil)			
Details of the Environmental Aspects (if More Than 5 critical aspect)			
Details of the OHSMS Significant RiSK (if More Than 5 critical OHSMS RiSK)			
Does your organization is not regulated by the law and don't need any license? ☐ YES ☐ NO			
Please write relevant laws applicable to your organization (Ex. air, water, waste, noise, chemical, mining, labour etc. laws), process related and product related legal requirement. (Mention the applicable requirements or provide the requirement of the documents)			
OHSMS risks associated with processes, the main hazardous materials used in the processes.			
Does your organization have any accident related to environment or OHSAS in recent 3 years? ☐ YES ☐ NO			
ISO 22000:2018 – Food Safety Management System – Additional Details			
1. Organization Details	Number of Sites to be Audited?		
	FSSAI License Registration No:		
2. FOOD SAFETY SYSTEM STATUS	Have you implemented HACCP Principles? ☐ YES ☐ NO		
	Total No. of HACCP Studies:		
	Any seasonality issues? ☐ YES ☐ NO		
	If yes, provide details separately: A. Product(s): B. Season/Months of operation: C. Peak production period: D. Impact on operations (volume/process variation):		
3. Production Details	How many process lines are there in production		
	Product Types:		
	Product Lines:		
	Product Development ☐ YES ☐ NO :		
4. Food Safety Controls	CCPs (Critical Control Points):		
	PRPs (Prerequisite Programs):		
	OPRPs (Operational PRPs):		
5. Infrastructure & Facilities	Building Area (in sq. ft./m²):		
	Infrastructure Details:		
	In-house Lab Testing Available? ☐ YES ☐ NO		

6. Audit History	Any prior audits conducted? ☐ YES ☐ NO	
	If yes, attach audit findings/report	
7. Additional Requirements	Translator Required? ☐ YES ☐ NO	
	Other Factors (specify):	

ISO 27001:2022 – INFORMATION SECURITY MANAGEMENT SYSTEM – ADDITIONAL DETAILS

1. SOA Version No. _ Date of implement: _____
 2. Any outsourced process (i.e., IT / Data Centre/Server) _____
 3. Have you done Risk Assessment & Risk Treatment, If yes on which date _____

Business complexity [Please select type of complexity in your org. as per A, B, C, chose any no. from 1 or 2 or 3]

A. Type(s) of business and regulatory requirements	1. Organization works in non-critical business sectors and non-regulated sectors; 02. Organization has customers in critical business sectors; 03. Organization works in critical business sectors.
B. Process and tasks	1. Standard processes with standard and repetitive tasks; lots of persons doing work under the organization's control carrying out the same tasks; few products or services 02. Standard but non-repetitive processes, with high number of products or services 03. Complex processes, high number of products and services, many businesses units included in the scope of certification (ISMS cover highly complex processes or relatively high number or unique activities).
C. Level of establishment of the MS	1. ISMS is already well established and/or other management systems are in place 02. Some elements of other management systems are implemented, others not 03. No other management system implemented at all, the ISMS is new and not established.

. IT complexity [Please select type of complexity in your org. as per A, B, C, chose any no. from 1 or 2 or 3]

A. IT infrastructure complexity	1. Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc 02. Several different IT platforms, servers, operating systems, databases, networks 03. Many different IT platforms, servers, operating systems, databases, networks
B. Dependency on outsourcing and suppliers, including cloud services:	1. Little or no dependency on outsourcing or suppliers 02. Some dependency on outsourcing or suppliers, related to some but not all important business activities 03. High dependency on outsourcing or suppliers, large impact on important business activities.
C. Information System development:	1. None or a very limited in-house system/application development 02. Some in-house or outsourced system/application development for some important business purposes 03. Extensive in-house or outsourced system/application development for important business purposes.

Confirmation of access to organizational records

01. Agreed to share all the ISMS records or information about design and effectiveness of controls for review by audit team.
 02. Not agreed to share all the ISMS records or information about design and effectiveness of controls for review by audit team, because it contains confidential or sensitive information.
 If you are "not agreed", please mention the information which cannot be shared in during the audit:

ISO/IEC 27701:2025 PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)– ADDITIONAL DETAILS

Business complexity [Please select type of complexity in your org. as per A, B, C, chose any no. from I or II or III or IV or V or VI]

A) Role of the organization (PII Controller / PII Processor)

What is the organization's role for each activity, product, or service within the PIMS scope?	PII Controller PII Processor Both PII Controller and PII Processor Not applicable (justified)
---	--

B) Identification of PII principals

Which categories of PII principals' data are processed for activities, products, or services within scope?	Employees Customers Suppliers / Vendors Contractors Website users / prospects Other (specify): _____
--	---

C) Statement of Applicability (SoA) – PIMS			
What is the current status of the organization's PIMS Statement of Applicability (SoA)?			SoA established and approved SoA version documented:----- - SoA reviewed and updated periodically SoA not established (nonconformity)
D) Confidential / Sensitive Information Availability			
Is any PIMS-related information (such as PIMS records or information on the design and effectiveness of controls) not made available to the audit team due to confidentiality or sensitivity?			No, all required information is available for audit review Yes, some information is restricted due to confidentiality or sensitivity Yes, information is restricted and alternative evidence has been provided Not applicable
E) PIMS Conformance to ISO/IEC 27701			
Does the client have a documented and implemented Privacy Information Management System (PIMS) that conforms to the requirements of ISO/IEC 27701?			Yes, PIMS is documented and implemented and conforms to ISO/IEC 27701 Partially documented / implemented (not acceptable for certification) No, PIMS is not documented and/or not implemented (application not acceptable)
PII Processing Risk Classification (For Audit Time Calculation) Select the applicable option(s): High / Medium / Low			
PII processing risks	Classification for audit time calculation		
	High Risk PII Processing	Medium Risk PII Processing	Low Risk PII Processing
Classification of PII	PII processing involves one or more of the following: Highly sensitive or special category PII Mandatory DPIA or similar risk assessment required Large volume of sensitive/special category PII PII of vulnerable individuals National identifiers (e.g., Aadhaar, NI number, passport) Bank account, financial or biometric information	PII processing involves one or more of the following: Large volumes of general PII including some special category data (e.g., HR data) Financial or identification data without large-scale exposure Pseudonymized PII that can be reversed to identify individuals Combination of multiple PII data sets	PII processing involves one or more of the following: General, non-sensitive PII Limited HR-related PII Encrypted PII with strong key management De-identified or anonymized data that cannot be reasonably re-identified
PII processing risks	High Risk PII Transfer	Medium Risk PII Transfer	Low Risk PII Transfer
Transfer of PII	Transfer of PII across multiple jurisdictions or countries Cross-border transfers without uniform legal frameworks Reliance on multiple transfer mechanisms	Transfer of PII within the same jurisdiction or aligned geographies Use of approved mechanisms (e.g., binding corporate rules, SCCs) Encryption used during PII transfer	No cross-border PII transfer PII processed and stored within a single jurisdiction Transfers limited to internal systems with controlled access
PII processing risks	High Complexity Processing	Medium Complexity Processing	Low Complexity Processing
Complexity of PII Processing	PII processing includes one or more of the following: PII profiling for commercial or behavioral purposes Data mining or large-scale analytics Automated decision-making affecting individuals Multiple regulations and legislations applicable Operations across multiple jurisdictions Multiple processes using different platforms and systems	PII processing includes one or more of the following: PII profiling for internal or operational purposes Sector-specific regulatory requirements Operations across multiple locations within the same jurisdiction Multiple processes using common platforms	PII processing includes one or more of the following: General, routine processing of PII Single operational location One or two simple processes Use of a single or limited number of platforms

Operational Risk Classification (For Audit Time Calculation) Select the applicable option(s): High / Medium / Low			
Operational Risk	High Operational Risk	Medium Operational Risk	Low Operational Risk
Number of Persons Processing / Accessing PII	Approximately 100% of personnel within the certification scope process or have access to PII	Approximately 50% to 75% of personnel within the certification scope process or have access to PII	Less than 25% of personnel within the certification scope process or have access to PII
Operational Risk	High Operational Risk	Medium Operational Risk	Low Operational Risk
Volume of PII Principal Data (Number of Records)	High volume of PII records (> 1 billion) Multiple independent PII data sets	Moderate volume of PII records (> 1 million) Limited number of PII data sets	Low volume of PII records (< 100,000) One or two PII data sets only
Operational Risk	High Operational Risk	Medium Operational Risk	Low Operational Risk
Number of ISO/IEC 27701 Annex A Controls Implemented (A.1, A.2, A.3)	All applicable Annex A controls (A.1, A.2, A.3) implemented	Approximately 70% of applicable Annex A controls implemented	Less than 30% of applicable Annex A controls implemented

ISO/IEC 42001:2023 Artificial Intelligence Management Systems (AIMS) – Additional Details

PLEASE SELECT THE APPLICABLE TYPE(S) OF COMPLEXITY BY TICKING THE APPROPRIATE OPTION

A. Availability of Documentation

Customer as a role: AI Producer and AI Customer or AI Provider & AI Customer

Is there any information can not be made available for review by the audit team because it content confidential or sensitive information?

YES, NO

Table B 1 — Classification of factors for adjustment of audit time

Factor for Adjustment of Audit Time	Normal Effort (✓)	Increased Effort (✓)
Number of regulatory frameworks within AIMS scope	Only one regulatory framework applies	More than one regulatory framework applies

High-risk or sensitive AI systems	No high-risk or sensitive AI use	AI systems involving safety, human rights, personal data, or critical decisions
Number of third-party agreements within AIMS scope	None or very few third-party agreements	Multiple third-party or outsourced AI service providers
Controls defined in Statement of Applicability (SoA)	Controls aligned only with ISO/IEC 42001 Annex A	Additional controls beyond ISO/IEC 42001 Annex A
For surveillance or re-certification audit		
Changes since last audit (for surveillance / recertification)	Minor or no changes to AIMS	Major changes in scope, AI systems, or governance
AI system lifecycle complexity	Simple lifecycle with limited changes	Frequent updates, retraining, or deployment changes
Organizational scale and structure	Single-site or centralized operations	Multi-site or distributed organizational structure
Data sensitivity and privacy exposure	Non-personal or anonymized data only	Personal, sensitive, or regulated data involved

Step 2 – Adjustment Factors (Based on Table B)

Adjustment Factor	Description	Additive Audit Time
Number of regulatory frameworks	Two regulatory frameworks applicable	
Number of AI systems	One AI system	
High-risk / sensitive AI purpose	Automotive (safety-critical)	
Third-party agreements	Two third-party providers	
Additional controls beyond ISO/IEC 42001	Two additional controls	

Step 3 – Total Audit Time Calculation

Description	Audit Days
Base audit time (from Table A)	
Total additional audit time	
Final audit time	Auditor days

ADDITIONAL INFORMATION'S OF SPECIFIC MANAGEMENT SYSTEMS (COMPLETE THE SECTION, IF APPLICABLE)

ISO 50001:2018 – Energy Management System – Additional Details

Annual Energy Consumption (Unit KWH etc.):		Number of EnMS Effective Personnels:	
Name & Number of Energy Sources:		Name & Number of significant energy uses (SEUs):	

ISO 37001:2016 – Anti Bribery Management System – Additional Details

Effective Number of employees under ABMS	
--	--

NOTE : Effective Number of Employees for ABMS shall include Personnels from Top Management, Governing Body, ABMS Compliance & Investigation Committee, Marketing, Purchase , Legal & Compliance, Due Diligence, Internal / External Audit, Finance & Accounts Departments.

ISO 37001:2016 – Anti Bribery Management System – Risks

Low (Financial and other Transition in limited business, Few stakeholders, no public delivery services, etc.)	
Medium (Financial and other Transition at larger Scale, Many stakeholders, no public delivery services, etc.)	
High (Financial & other Transition at larger Scale, National, International & Government bodies stakeholders, Public delivery services, etc.)	

ISO 21001:2018 – Educational Organizations Management System – Effective Number of employees under EOMS

staff employed by the organization;(Including Academic and Non-Academic)	
volunteers and interns working with or contributing to the organization;	
staff of external providers working with or contributing to the organization.	
Other Supporting staff like: (admin, support, maintenance, canteen, etc)	
TOTAL	0

ISO 21001:2018 – Educational Organizations Management System – Risks

Low (Coaching and Entrance exam preparation Centres & Institutes Educational organizations — Management systems, etc.)	
Medium (All Educational school under State, Central Government approved through concern Educational Bords (national or international) All other types of business sectors not covered under High or Low Risks)	
High (Management Courses Institutes (national or international) Technical Courses Institute (national or international) University and Professional Courses Institutes (national or international), etc.)	

ANNEXURE -01 IN CASE OF MULTI-SITE								
No. of Employees	Total				Contractual	0	Working No. of Shifts	0
Activities	Full Time	Part time	Performing Same type of Job	Temporary Unskilled workers	Effective No. of Employees, Filled by Q4A			
Management								
Production Area/Service								
Quality Control/Technical								
Administration								
Other								
Operation for Weekend / weekly holiday:								
A representative number of sites have been sampled by the Q4A, taking into account:								
1) the results of internal audits of the central office (if appropriate) and the sites;								
2) the results of management review;								
3) variations in the size of the sites;								
4) variations in the business purpose of the sites;								
5) complexity of the information systems at the different sites;								
6) variations in working practices;								
7) variations in activities undertaken;								
8) variations of design and operation of controls;								
9) potential interaction with critical information systems or information systems processing sensitive information;								
10) any differing legal requirements;								
11) geographical and cultural aspects;								
12) risk situation of the sites;								
13) information security incidents at the specific sites.								
Please write the below answers:								
A-are same corporate?								
B-are actually implementing same activity in control?								
C-have same CEO?								
D-are using same quality system and procedure?								
* Please attach detail information about multi-site (Total site no./size and location of each site)								
No. of Employees							0	
In case, if you have more site's, kindly fill this annexure per site.								
Date:		Representative Name	0					
REVIEW (TO BE FILLED BY Q4A MANAGEMENT FZE LLC)								
Acceptance, Ref. No		Not Acceptance-----						
Supplement information, if needed: -----								
Q4A MANAGEMENT FZE LLC AUD-F-02-Request for Proposal cum Application Form/ Rev.: 05								