



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



# **Selection of ISO27001 & ISO27701 Audit Company/Firm**

**(LOT #2)**

**March 2023**

**Pakistan Software Export Board (Guarantee) Limited**

**Ministry of Information Technology & Telecom**



# GDPR Compliance of IT/ITeS Companies Through ISO27001 & ISO27701 Certifications



## Table of Contents

Introduction .....	1
Terms of Reference.....	2
Key Objectives.....	2
Responsibilities of the Audit Firm.....	2
Deliverables for the Assignment.....	2
Duration of Assignment .....	2
Eligibility/ Evaluation Criteria of Audit Company/Firm.....	3
Financial Evaluation Scoring Criteria.....	5
Bid Evaluation Terms .....	5
Bid Submission Guidelines .....	5
FORM TECH 1 – PROPOSAL SUBMISSION COVER LETTER.....	5
FORM TECH 2 – BIDDER’S INFORMATION .....	7
FORM TECH 3 – BIDDER’S EXPERIENCE AS ISO AUDITOR/CERTIFICATION BUSINESS .....	8
FORM TECH 4 –LIST OF NATIONAL AND INTERNATIONAL CLIENTELE OF BIDDING COMPANY/FIRM IN ISO27001/ISO27701 CERTIFICATIONS .....	9
FORM TECH 5– LIST OF LEAD AUDITORS .....	10
FORM TECH 6 – FORMAT OF CURRICULUM VITAE (CV) OF LEAD AUDITORS.....	11
FORM TECH 7 – WORK BREAK DOWN-STRUCTURE OF LEAD AUDITORS .....	12
FORM TECH 8 – LIST OF ISO27001/ ISO27701 AUDITS CONDUCTED BY THE LEAD AUDITOR.....	13
FORM FIN 1 – FINANCIAL PROPOSAL STANDARD FORM.....	14
FORM FIN 2 – AUDITS COST .....	15



## **GDPR Compliance of IT/ITeS Companies Through ISO27001 & ISO27701 Certifications**



### **Introduction**

Pakistan Software Export Board (PSEB), Ministry of Information Technology is the apex body of the Ministry of Information Technology, Government of Pakistan, to provide an enabling environment and take measures for the growth of Information Technology / Information Technology Enabled Services (IT/ITES) exports and thus support IT/ITES industry. In this respect, PSEB is providing support to the local IT/ITES companies in reaching out to their potential clients abroad, attracting and facilitating foreign IT/ITES firms to establish their development facilities in Pakistan. PSEB also arranges the participation of the Pakistani IT/ITES Industry in domestic and international IT/ITES events, and provides protocol, hosting, and match-making facilities for foreign delegates and investors with the purpose to accelerate the growth of IT/ITES exports.

With the implementation of the European Union's General Data Protection Regulation (GDPR) on May 25, 2018, a new regulatory regime for business in Europe and beyond is becoming more and more challenging, especially for Pakistani IT companies. Governments outside Europe are introducing new data-protection regulations or enhancing existing rules to make them compliant with the GDPR to retain and expand business in the EU region.

In a major step towards ensuring sustainable growth of Pakistan's IT/ITES industry in the European Market, Pakistan Software Export Board (PSEB) intends to facilitate IT/ITeS companies to comply with European Union's General Data Protection and Regulation (GDPR) compliance which is adopted by the European Parliament to do business in Europe. The most cost-effective way to comply with GDPR is by achieving ISO27001 and ISO27701 certifications. Implementing both ISO 27001 and ISO 27701 certifications and some additional controls will enable businesses to meet the EU GDPR's requirement for "appropriate technical and organizational measures", as well as help them to comply with many other data protection regulations.

PSEB aims to certify (50) IT/ITES companies on ISO27001 and ISO27701 standards in the next two years for the purpose of GDPR compliance. PSEB shall bear 70% of the consultancy and audit cost of ISO27001 and ISO27701 certifications and 30% will be paid by the selected IT/ITeS companies. The successful implementation of the proposed project would give the Pakistan IT industry global recognition as a front-liner country in implementing data security and complying with GDPR regulations for enhancing IT exports to the EU in particular.

**For the purposes of execution of this project, PSEB intends to select an ISO auditing firm to provide ISO27001&ISO27701 audit services to 25 IT/ITeS companies in Lot-2. The bidder selected in one lot will not be eligible to participate in the subsequent lot.**



## GDPR Compliance of IT/ITeS Companies Through ISO27001 & ISO27701 Certifications



### Terms of Reference

#### Key Objectives

The key objectives of this assignment are mentioned as follows:

Key Objectives
To conduct an audit of 25 IT/ITeS companies on ISO27001 and ISO27701 standards and issuance of an accredited certificate to the certified companies

#### Responsibilities of the Audit Firm

The audit firm will be responsible for the following:

S. No.	Responsibilities of the Company/Audit Firm
1	To conduct audit of 25 IT/ITeS companies on ISO27001 and ISO27701 standards
2	Pre-assessment and document review of 25 IT/ITeS companies for audit
3	To conduct a stage-1 audit to identify any major areas of concerns for compliance
4	To conduct a stage-2/final audit and provide accredited ISO27001&ISO27701 certificates to successful audited IT/ITeS companies

#### Deliverables for the Assignment

The deliverables of this assignment are mentioned as follows:

S. No	Deliverables
1	Conduct pre-assessment of IT/ITeS companies who have qualified consultancy stage and submit an audit plan with timelines for successful completion of stage-1 and stage-2 audit
2	Conduct Stage-1 Audit and submission of audit Report of the IT/ITeS company
3	Conduct Stage-2/final Audit and submission of audit Report of the IT/ITeS company
4	Issuance of accredited ISO27001&ISO27701 certificates to the certified IT/ITeS companies

#### Duration of Assignment

The expected duration of each assignment is within 30 calendar days per company. However, the Applicant firm is encouraged to propose a shorter duration for the assignment, without compromising the quality of deliverables.



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



## Eligibility/ Evaluation Criteria of Audit Company/Firm

PSEB shall evaluate the technical proposals in line with the following evaluation criteria. The technical evaluation of only those bidders will be carried out who qualifies the mandatory part of the technical evaluation.

### Mandatory Requirements for Eligibility

Technical Bids must have the following documents attached to be considered eligible for further technical evaluation:

S #	Item Description	Documents/Proof
1	The bidding company/firm must be in the ISO audit/certification business for at least last 03 years.	<ol style="list-style-type: none"><li>1. Incorporation documents of the bidding firm/company.</li><li>2. Detailed profile of the Company/Firm</li><li>3. List of verifiable clients already audited and certified by the company on different ISO standards as per Tech Form-3.</li></ol>
2	The bidding firm shall provide accredited ISO27001&ISO27701 certifications itself or shall have affiliation/authorization/partnership with an international firm that can provide accredited ISO27001&ISO27701 certifications by a full member of the International Accreditation Forum (IAF).	<ol style="list-style-type: none"><li>1. Letter/Proof from the international firm/company for its local affiliation/ authorization/partnership for conducting ISO27001&amp;27701 audits in Pakistan.</li><li>2. Proof of valid ISO27001&amp;ISO27701 accreditation from a full member of IAF.</li></ol>
3	The bidding company/firm must possess valid NTN and General Sales Tax (GST) Registrations and have Active Tax Payer status.	Copies of Income Tax & Sales Tax Registration Certificates.
4	The bidding company/firm must provide an Affidavit that it is not blacklisted and involved in any active litigation against the Government of Pakistan.	Notarized Affidavit by Company/firm on PKR 100 stamp paper



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**Detailed Technical Evaluation Scoring Criteria**

The detailed technical evaluation would be based on the bidder’s capability. The detailed technical evaluation will be performed by the Procurement Committee and marks given as per the following scoring criteria:

**Detailed Technical Evaluation Scoring Matrix**

Serial No.	Scoring Criteria for Bidders	Marks	Technical Form
<b>1</b>	<b>Company/Firm Profile and Experience</b>	<b>60</b>	
I	1. Bidding company/firm Experience in ISO audit/certifications. Marking scheme for this criterion: 5 Years or more with minimum 20 certified clients – 10 marks 4 Years with minimum 15 certified clients – 08 marks 3 Years with minimum 10 certified clients – 06 marks Less than 03 Years and less than 10 clients– No Marks	10	Tech 3
II	The list of national and international clientele of bidding company/firm who have been certified on accredited ISO27001/ISO27701 standards. (01 certified client = 2.5 Mark) (Less than 05 Completed Certifications = No Marks)	50	Tech 4
<b>2</b>	<b>Qualification and Experience of Lead Auditors</b>	<b>40</b>	
I	1. The bidding company/firm shall have a minimum of 02 lead auditors on its auditors’ pool. Each auditor must have completed 16 years of education and shall be an ISO27001/ISO27701 certified Lead auditor from CQI-IRCA and must have conducted 02 ISO27001/ISO27701 audits.  (01 Lead Auditor = 05 Marks and Maximum 20 Marks, less than 02 Lead Auditors=0 Marks) <b>Note 1:</b> (Please attach copies of each Lead auditor’s 16 years’ educational certificate/degrees and ISO27001/27701 certificates. No marks shall be given without proof of required documents) <b>Note 2:</b> (A detailed work breakdown structure of Lead Auditor as per Tech 7 and 01 Lead Auditor will complete a minimum of 06 audits.)	20	Tech 5 Tech 6 Tech 7
	2. Number of ISO27001/ISO27701 audits conducted by lead auditors. (01 completed audit = 0.5 Mark and Maximum 05 Marks for 01 lead auditors and 20 Marks in this section)	20	Tech 8
	<b>TOTAL TECHNICAL EVALUATION SCORE</b>	<b>100</b>	



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



## **Financial Evaluation Scoring Criteria**

The financial scores will be awarded on a proportionate basis, with the lowest-priced compliant bid getting the highest marks. Provide your financial bids in the attached format from Fin 1 and Fin 2.

### **Bid Evaluation Terms**

1. Any applicant, not fulfill mandatory requirements will be outrightly rejected and not included in technical evaluation.
2. The companies securing 60% or above marks in technical evaluation will be invited for the opening of financial bids.
3. The financial bids will be opened in the presence of the authorized representatives of the bidder.
4. The financial bids will then be evaluated by PSEB to check their compliance and calculations of total amounts.
5. The final score will be calculated for compliant firms as follows:

Final Score of Firm = Technical Score \* 60% + Financial Score \* 40%

### **Bid Submission Guidelines**

1. Single stage two envelope process will be followed.
2. Each proposal shall be submitted as two printed copies (one marked as ORIGINAL & one as COPY). A softcopy may also be attached with the proposal.
3. Technical and Financial proposals must be sealed separately and clearly marked as Technical Proposal & Financial Proposal for ISO27001&ISO27701 audit services.
4. Financial proposal must be accompanied by bid money (refundable) @ 2% of the Financial Bid Amount (inclusive of all applicable taxes) in the form of a Pay Order/Demand Draft in favor of "PSEB" (cheques will not be accepted).
5. Advance payments if requested shall be made only against an equal amount of unconditional bank guarantee from a first-class Pakistani bank to the satisfaction of PSEB authorities.
6. All required documents must be attached with the bid and if any required document is not found with the proposal, PSEB reserves the right to reject the proposal at its discretion.
7. 5% performance guarantee shall be submitted by the successful bidder in the form of either an unconditional bank guarantee from a first-class Pakistani bank or Pay-order and shall be released after completion of work to the satisfaction of PSEB authorities.

### **Contact Information:**

**Mr. Shoaib Sarwar**

**Project Manager**

Pakistan Software Export Board

6th Floor, New State Life Tower

Plot No #61 Jinnah Avenue, Islamabad.

Phone 051-9212368



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 1 – PROPOSAL SUBMISSION COVER LETTER**

To

**Director Projects**

Pakistan Software Export Board  
6th Floor, New State Life Tower  
Plot No #61 Jinnah Avenue, Islamabad.  
Phone 051-9212368

Dear Sir,

We, the undersigned, offer to act as an ISO auditing firm for services of ISO27001&ISO27701 audits to the 25 IT/ITES companies, in accordance with your Request for Proposal dated [Insert Date] and our Proposal. We are hereby submitting our Proposal, which includes this Technical Proposal and a Financial Proposal sealed under a separate envelope.

We declare that all the information and statements made in our proposals are true and accept that any misinterpretation contained in them may lead to our disqualification.

Our proposals are binding upon us.

We understand you are not bound to accept any proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: [insert]

Name of Firm: [insert]

Address: [insert]





**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 2 – BIDDER’S INFORMATION**

All individual Bidders are requested to complete the information in this form.

<b>Sr. No</b>	<b>Description</b>	<b>Response</b>
1	The legal name of the bidder	
2	Nature of Business: (Whether the firm is a Corporation, Partnership etc.)	
3	Head Office and sub-office Address	
4	Place of Incorporation / Registration	
5	Year of Incorporation / Registration	
6	Name of the CEO	
7	Applicant’s authorized representative	
8	Telephone numbers	
9	Fax numbers	
10	E-mail address	
11	Number of Employees	



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 3 – BIDDER’S EXPERIENCE AS ISO AUDITOR/CERTIFICATION BUSINESS**

Each audit/certification assignment shall only be evaluated for scoring if a copy of the ISO certificate is attached.

<b>Sr. No</b>	<b>Clients’ Contact Details (Name, address, phone, and email)</b>	<b>Country</b>	<b>Name of ISO Standard</b>	<b>Month and Year of Completion ISO Audit</b>	<b>Verifiable copy of Accredited ISO Certificate</b>



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 4 –LIST OF NATIONAL AND INTERNATIONAL CLIENTELE OF BIDDING  
COMPANY/FIRM IN ISO27001/ISO27701 CERTIFICATIONS**

Each audit assignment shall only be evaluated for scoring if a copy of the ISO27001/ISO27701 certificate is attached.

<b>Sr. No</b>	<b>Clients' Contact Details (Name, address, phone, and email)</b>	<b>Country</b>	<b>Month and Year of Completion of Audit</b>	<b>Verifiable copy of Accredited ISO27001/ ISO27701 Certificate</b>



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 5– LIST OF LEAD AUDITORS**

Name	Experience	Qualification/ Degree	ISO Certifications

(Please attach copies of the 16 years' educational certificate/ degrees and copies of ISO27001/27701 certificates. No marks shall be given without proof of documents)



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 6 – FORMAT OF CURRICULUM VITAE (CV) OF LEAD AUDITORS**

**Name of Firm** [*Insert name of firm proposing the staff*]: \_\_\_\_\_

**Name of Staff** [*insert full name*]: \_\_\_\_\_

**Date of Birth:** \_\_\_\_\_

**Nationality:** \_\_\_\_\_

**Educational Qualification:** [*Summarize college/university and other specialized education of staff member, giving names of schools, dates attended and degrees obtained*]:

**ISO27001&ISO27701 Certifications:**

**Countries of Work Experience:** [*list countries where staff has worked*]:

**Employment Record:**

[*Starting with present position, list in reversed order, every employment held by staff member since graduation, giving for each employment (see format here below): dates of employment, name of employing organization, position held*]:

From [Year]: To [Year]:

Employer:

Position held:



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 7 – WORK BREAK DOWN-STRUCTURE OF LEAD AUDITORS**

<b>Name of Lead Auditor</b>	<b>Number of Companies to be certified audited/certified on accredited ISO27001/ISO27701 standard</b>

1. M/s -----(bidding firm name) hereby confirms that the above-named auditors shall provide ISO27001/ISO27701 auditing services as per the number of companies mentioned in Tech form-7. We also confirm that we shall take prior approval from PSEB if any Lead Auditor is changed and shall share all the technical and financial information related to the newly appointed Lead auditor to PSEB for the record.

2. M/s -----(bidding firm name) remains committed to ensuring compliance with the responsibilities and sharing deliverables of assignment in the designated time frame.



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM TECH 8 – LIST OF ISO27001/ ISO27701 AUDITS CONDUCTED BY THE LEAD  
AUDITOR**

<b>Sr. No</b>	<b>Clients' Contact Details (Name, address, phone, and email)</b>	<b>Country</b>	<b>Date of Completion of Work</b>	<b>Verifiable evidence of conducting Accredited ISO27001/ISO27701 Audit</b>



**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM FIN 1 – FINANCIAL PROPOSAL STANDARD FORM**

To

Director Projects  
Pakistan Software Export Board  
6th Floor, New State Life Tower  
Plot No #61 Jinnah Avenue, Islamabad.  
Phone 051-9212368

Dear Sir,

We, the undersigned, offer to provide the ISO27001&ISO27701 auditing services to **PAKISTAN SOFTWARE EXPORT BOARD (GUARANTEE) LIMITED** in accordance with your Request for Proposal dated [Insert Date] and our Technical Proposal. Our attached Financial Proposal is for the sum of [Insert amount(s) in words and figures] for 25 companies.

Our Financial Proposal shall be valid for 90 days from the date of submission of proposal.

Yours sincerely,

Authorized Signature [In full and initials]: \_\_\_\_\_

Name and Title of Signatory: [insert]

Name of Firm: [insert]

Address: [insert]





**GDPR Compliance of IT/ITeS Companies  
Through ISO27001 & ISO27701  
Certifications**



**FORM FIN 2 – AUDITS COST**

	A	B	C
Description	Small Size Company (10-50 Employees) (Rs.)	Medium Size Company (51-100 Employees) (Rs.)	Large Size Company (100+ Employees) (Rs.)
A) ISO27001 Audits			
B) ISO27701 Audits			
<b>Total cost per company (A+B)</b>			
<b>Number of companies</b>	5	15	5
<b>Total cost for a number of companies under each category</b>			
<b>Total cost/value of bid for 25 companies</b>			

1. Bidder is required to quote its total fee including all out-of-pocket expenses in the format shown above.
2. All Government taxes should be included in the price.