

# Request for Quotation: Engagement of Cyber Security Audit Services Provider



Document No: aitpl/217/2024-25  
Last date of response submission:  
31<sup>st</sup> Oct 2024



## Contents

1.	DEFINITIONS .....	3
2.	INTRODUCTION AND BACKGROUND.....	3
2.1	INTRODUCTION .....	3
2.2	ABOUT AABSYS IT .....	3
3.	RFQ QUESTIONS .....	4
4.	LAWS AND REGULATIONS.....	4
5.	COSTS INCURRED IN RESPONDING TO THE RFQ .....	4
6.	DISCLOSURE REQUIREMENTS.....	4
7.	ELIGIBILITY CRITERIA .....	4
8.	QUESTIONNAIRE AND WRITTEN RESPONSES .....	5
9.	SUBMISSION OF RESPONSES .....	6
9.1	GENERAL INSTRUCTIONS FOR SUBMISSION OF RESPONSES .....	6
9.2	OTHER REQUIREMENTS .....	6
10.	SELECTION CRITERIA .....	7
11.	TECHNICAL SPECIFICATIONS .....	7
11.1	OBJECTIVE OF THE PROJECT.....	7
11.2	GENERAL REQUIREMENTS.....	8
11.3	TECHNICAL REQUIREMENTS .....	8
12.	DELIVERABLES.....	9
12.1	GENERAL DELIVERABLE REQUIREMENTS.....	9
12.2	EXPECTED OUTPUT .....	9
13.	TIMELINES.....	10

## 1. Definitions

Following are the acronyms used in this document, and their definitions:

Acronym	Definition
API	Application Programming Interface
Auditee	Department or Owner of the application who is facing the audit or assessment
BID	Bug Track ID
CERT	Computer Emergency Response Team
CISA	Certified Information System Auditor
CISSP	Certified Information System Security Professional
RFQ	Request for Quotation
SI	System Integrator
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SPOC	Single Point of Contact
SQL	Structured Query language
SSO	Single Sign-on Computing
VA/PT	Vulnerability Assessment/Penetration Testing
WASA	Web Application Security Assessment

## 2. Introduction and Background

### 2.1 Introduction

AABSyS IT is seeking proposals from CERT-In Empaneled Information Security Auditing Organizations for Risk Assessment, Security Audit, and Incident Response Planning Services This RFQ details the eligibility criteria for the selection of the service provider, the scope of services that are to be performed, and the timelines for the selection process.

### 2.2 About AABSyS IT

AABSyS IT is a 26-year-old, award-winning company that leverages digital technologies, deep domain expertise, strong financials, and scaling-up expertise to provide cutting-edge geospatial, IT, and engineering services to global customers, and helps them stay ahead of the curve. The company brings together deep domain expertise, talented personnel, and rich experience to meet a variety of customer needs in geospatial and IT services. The company has an established state-of-the-art infrastructure and world-class facilities in Bhubaneswar and at Tier 3 locations - Berhampur and Balasore, in Odisha, along with a global sales office located in the Delhi-NCR region. One of the key strengths of AABSyS is its rich experience, expertise, and exposure to web application development. The company has a track record of supporting some of the prestigious customers in Europe, Australia, and the US, for GIS and CAD solutions, software automation, and offshore GIS software development projects, in a diverse set of software technologies and platforms.

AABSyS has its core competencies in the areas of geographic information system (GIS), computer-aided drafting (CAD), computer-aided facility management (CAFM), remote sensing, photogrammetry, and software development, such as in GIS-based application

development with solutions for natural resource management, urban planning, environment, utility, and e-governance.

AABSyS IT continuously seeks to achieve excellence in all aspects of its operations. Our operations, processes, systems, and work environment are periodically reviewed and enhanced through ISO 9001, ISO 14001, ISO 27001, ISO 45001, and CERT-In VPAT certifications. The company has adopted these standards to provide global clients with the highest levels of GIS and CAD services, software development processes, and information security.

### 3. RFQ Questions

Questions concerning this RFQ should be directed to the Head of the IT Department by email, as detailed under **Section 8** of this RFQ. AABSyS IT will publish a consolidated response to all questions received, which will be emailed to all bidders of this RFQ.

### 4. Laws and Regulations

All applicable laws of the Republic of India, and state laws of Odisha, shall apply to this RFQ.

### 5. Costs Incurred in Responding to the RFQ

All expenses, whether direct or indirect, associated with preparing a response to the RFQ or presentations required to support or clarify the proposal, as requested by AABSyS IT, shall be fully borne by the bidders.

### 6. Disclosure Requirements

The bidder must disclose to AABSyS IT any known or reasonably anticipated conflicts of interest related to the firm's provision of services to AABSyS IT. Additionally, the firm must disclose any legal or disciplinary events that may be relevant to AABSyS IT's evaluation of the firm or the integrity of its management or advisory personnel.

### 7. Eligibility Criteria

S. No.	Basic Requirement	Eligibility Criteria	Documentary Proof to be submitted
1	CERT-IN	The bidder must be CERT-IN empaneled agency	CERT-IN registration Number.
2	Legal Entity	<ul style="list-style-type: none"> <li>▪ The bidder should have conducted business in India for the past three (3) financial years.</li> <li>▪ The Bidder shall be solvent at the date of Bidding</li> <li>▪ The Bidder shall have positive net worth</li> </ul>	<ul style="list-style-type: none"> <li>▪ Certificates of incorporation for Company/ Partnership Deed / Proprietorship firm self-declaration</li> <li>▪ Certificate from Statutory auditor / Chartered Accountant for the existence of the firm for the last five years along with the last three years'</li> </ul>

			<p>balance sheet.</p> <ul style="list-style-type: none"> <li>▪ Certificate from Statutory auditor / Chartered Accountant for Solvency</li> </ul>
3	Work Experience	The Bidder should have executed at least 8 orders of similar nature of jobs, particularly in Cyber Threat & Vulnerability Assessment and Site Security Audit Services.	Copy of letter of award / Work Order or Certificate of Completion, with a detailed scope of work from clients of the bidder, shall be provided.
4	Other legal documents	<ul style="list-style-type: none"> <li>▪ GST Certificate</li> <li>▪ Income Tax Return (Last 3 years)</li> <li>▪ PAN</li> <li>▪ Articles of Association/</li> <li>▪ Company Registration Certificate</li> </ul>	Copy of the valid documents attested by the authorized signatory
5	Blacklisting	The bidder must not be blacklisted by any Central/ State Department /establishments in India at any point in time due to breach of ethical conduct or fraudulent practices.	<p>A self-declaration that the bidder has not been blacklisted is to be submitted.</p> <p>In case it is found after issuing the Work Order that the concerned organization is blacklisted by any Central/ State Department /establishment in India, the work order will be cancelled.</p>

## 8. Questionnaire and Written Responses

Bidder shall provide written responses to each of the following questions reproducing the original question with each answer.

1. Describe the Bidder’s experience in the information technology subject matter areas and include descriptions of projects within the last three years.

Name of Client	Dates of Service	IT Subject Matter Area	Type of Work Performed (e.g. Audit, Non-audit, other services)

2. Describe the Bidder’s experience evaluating governance, risk management, and controls in general about the information technology subject matter areas.
3. Describe the Bidder’s experience and knowledge of control frameworks and standards about the information technology subject matter areas.
4. Describe relevant industry certifications maintained by personnel anticipated to lead and manage future internal audit projects with AABSyS for information technology subject matter areas.

## 9. Submission of Responses

### 9.1 General Instructions for Submission of Responses

- Bidders can submit their responses to the RFQ through email in the following format:

Subject: Response from <Vendor name> for Engagement of Cyber Security Audit Services Provider

The Technical and Financial bids must be enclosed as separate documents with the heading “Engagement of Cyber Security Audit Service Provider” to the official below:

The Head of the Department  
Information Technology Division  
AABSyS IT Private Limited  
Email: [it.admin@aabsys.com](mailto:it.admin@aabsys.com)

- Documents should be prepared in PDF format and enclosed in three separate attachments:
  - **Attachment 1: Documentary Evidence**  
This attachment should contain all documents supporting the eligibility criteria detailed under **Section 7** of this RFQ.
  - **Attachment 2: Technical Proposal**  
This attachment should contain the Technical Proposal and responses to questions.
  - **Attachment 3: Financial Proposal**  
This attachment should contain the financial proposal.
- Bidders can raise their queries regarding the RFQ process or seek clarifications through email with the following subject line to The Head of the IT Department [it.admin@aabsys.com](mailto:it.admin@aabsys.com) :

Subject: Pre-bid Query from <Vendor name> for Engagement of Cyber Security Audit Services Provider

### 9.2 Other Requirements

- The financial proposal should detail the costs incurred per month and should have a monthly milestone-based billing plan.
- GST should be mentioned extra, in line with the regulations of the Govt. of India.

AABSyS shall have the right to select the agency without assigning any reasons.

## 10. Selection Criteria

The following criteria will be used to evaluate proposals received:

- Bidder's Qualifications and Experience (50%)

This criterion includes the ability of the Bidder to meet the terms of the RFQ, and any special considerations, which the Bidder feels may increase its ability to perform the contract. Within this criterion consideration will be given to:

- Expertise: level of capability to perform the services required
- Quality of performance; professional qualifications of the key personnel assigned relevant to the work to be performed
- Experience, within the last five (5) years, providing the same or substantially similar services as outlined in this RFQ for other entities, preferably in the IT or IT-Enables Services (ITeS) sector
- Reputation, ethical standards, and disciplinary history such as judgments or sanctions
- Feedback from three references with at least one from an IT or ITeS customer of similar scope and size

- Understanding the needs of AABSyS IT (30%)

This factor refers to the extent to which the Bidder's proposal reflects its:

- Understanding of AABSyS IT's external audit needs and objectives.
- Understanding of the nature and scope of the work involved.
- Accessibility and responsiveness.

- Reasonableness of Costs (20%)

These points will be awarded based on the cost and efficiency of the Bidder's proposed approach. Efficiency and economy are very important to AABSyS IT, but this area will not necessarily be the primary deciding factor in the selection process.

Shortlisted companies shall be invited to present their solution to AABSyS IT.

## 11. Technical Specifications

### 11.1 Objective of the Project

AABSyS IT seeks to engage a third-party auditing agency from the CERT-In empaneled Information Security Auditing Organizations. The primary goal of this project is to comprehensively review the security implementation across our various web-based applications. The selected agency will conduct vulnerability assessments, identify potential weaknesses, and provide actionable recommendations. This initiative represents a crucial step toward ensuring a cyber-safe environment for AABSyS IT.

## 11.2 General Requirements

- The successful Contractor will provide specialized skills, industry, and subject matter knowledge in information technology to assist the CAE and Internal Audit staff.
- The selected Contractor may perform audit services in an outsourced arrangement. This project may also include a “knowledge transfer” component for training and assisting AABSyS IT Internal Auditors in the performance of engagement procedures. The Contractor may participate in all or some of the phases of an engagement, including planning and risk assessment, conducting fieldwork and testing controls, and developing recommendations to improve AABSyS business processes and mitigate risks.
- The Head of the IT Dept. will be responsible for approving the Contractor’s project plan for engagement as well as the objective and scope of procedures or services to be conducted. Deliverables will be determined by the objective and scope of each engagement and will be directly provided to the Head of the IT Dept. for approval.

## 11.3 Technical Requirements

The contractor may evaluate risks and administrative, technical (logical), physical, and organizational controls for the security of data and information that includes security vulnerability assessment and management in the following manner:

### Risk Assessment

- Conduct a comprehensive risk assessment to identify vulnerabilities in our systems.
- Assess the effectiveness of existing controls and evaluate the adequacy of existing security protocols
- Formulate responses and action plans including the mitigation, transfer, and avoidance of risk
- Provide a detailed report with recommendations for risk mitigation.

### Security Audit

- Perform a security audit of existing policies, procedures, and technologies.
- Evaluate compliance with relevant regulations and standards (e.g. VAPT, GDPR, HIPAA, SOC2 TYPE 1 & 2).
- Assess the vulnerabilities present in AABSyS systems, applications, and networks
- Evaluate backup frequency, data retention policies, and disaster recovery plans

### Incident Response Planning

- Develop or enhance an incident response plan tailored to our organization.
- Conduct tabletop exercises to test the effectiveness of the plan.
- Undertake documentation for Cyber-threat Preparation, Incident Detection, and Incident Response Threshold Determination
- Define the Threat Management and Containment Processes
- Formulate a fast and effective Recovery Plan and procedure for Post-Incident Review



### **Security Awareness Training**

- Provide training programs for employees on cyber security best practices.
- Customize the training content based on the specific needs and concerns of employees
- Devise some engaging delivery methods for training, such as videos, interactive sessions, quizzes, etc.
- Assess the effectiveness of training through follow-up evaluations.

### **License Audit**

- Review internal software license policies and procedures to ensure alignment with vendor contracts and compliance requirements
- Gather information about license keys, usage metrics, and deployment patterns.
- Evaluate the compliance levels with the terms and conditions set forth by software vendors.
- Recommend remediation steps

### **Reporting and Documentation**

- Deliver regular reports on security status, incidents, and compliance.
- Maintain documentation of all processes and findings.

## **12. Deliverables**

### **12.1 General Deliverable Requirements**

- The requirements and specifications for each deliverable in each engagement shall be defined and approved in writing by the Contractor before work is initiated, including the evaluation criteria for successful completion and quality assurance.
- The contractor should submit a timeline for each deliverable in consultation with the IT Dept., and the overall engagement shall be reviewed on a regular basis.
- Deliverables shall be provided on the dates specified. Any changes to the delivery dates must have prior written approval by the IT Dept.

### **12.2 Expected Output**

- Comprehensive risk assessment report.
- Security audit report with actionable recommendations.
- Documentation for Cyber-threat Preparation, Incident Detection, and Incident Response Threshold Determination
- Incident response plan along with a recovery procedure for Post-Incident Review
- Security Awareness Training Plan and content, with recommendations
- Monthly/quarterly security status report.

### **13. Timelines**

Bidders must adhere to the following timelines for this RFQ:

- RFQ Release: 17<sup>th</sup> October 2024
- Pre-bid query submission: 21<sup>st</sup> October 2024
- Pre-bid meeting: 22<sup>nd</sup> October 2024
- Proposal submission deadline: 31<sup>st</sup> October 2024
- Technical Presentation: To be intimated directly to the shortlisted bidder
- Announcement of Results: To be intimated later



- Deep domain expertise and rich experience in end to end GIS, CAD and Software services
- Partner-centric business approach with 70% repeat business
- Preferred services provider to prestigious companies in UK, Europe, Australia and US
- Six sigma-based quality management processes
- Innovative mix of onshore and offshore delivery model
- Winner of STPI Award of Excellence
- Winner of State Export Awards, Odisha

For more information visit our website:

[www.aabsys.com](http://www.aabsys.com)