



**Request for Proposal for the selection of Implementation of the IIMB Shield  
2026 for the Indian Institute of Management Bangalore.**

IIMB/IT/2025-26/01  
Date: 12/05/2026

## DISCLAIMER

The information contained in this Tender document or subsequently provided to Tenderers, whether in document or verbal or any other form by or on behalf of Indian Institute of Management, Bangalore (IIMB) by any of its employees or advisors, is provided to Tenderers on the terms and conditions set out in this Tender document and such other terms and conditions subject to which such information is provided.

The purpose of this Tender document is to provide interested parties with information that may be useful to them in eliciting their quotations pursuant to this Tender document. This Tender document may not be appropriate for all persons, and it is not possible for the Institute, its employees, or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this Tender document.

This Tender document includes statements which reflect various assumptions and assessments made by the Institute in relation to the Contract. Such assumptions, assessments and statements do not purport to contain all the information that each Tenderer may require.

The assumptions, assessments, statements, and information contained in this Tender document may not be complete, accurate, adequate, or correct. Each Tenderer should, therefore, conduct his/her own investigations and analysis and should check the Accuracy, Nature, Uniformity, Dependability, Exactness, Essence, and Precision of the assumptions, assessments, statements, and information contained in this Tender document, and obtain independent advice from appropriate sources.

Information provided in this document to the Tenderer(s) is on a wide range of matters, some of which depend upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The Institute accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. In the event of any ambiguity or doubt as regards the Tender Documents or inconsistency or conflict as between the provisions of the Tender Documents, the interpretation placed by IIMB shall be final and binding on the Bidders / Tenderer.

Institute, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Tenderer under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender document or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender document and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender document or arising in any way in this Tender Stage.

### **Caution Notice**

The Tender Inviting Authority (TIA), IIMB does not solicit or demand any money, fees, commission, gratification, or consideration of any kind from bidders or prospective bidders in connection with this tender.

However, EMD(if applicable) should be submitted as mentioned in the tender document.

Bidders are hereby cautioned that any person claiming to act on behalf of the TIA or the Institute and seeking money or any other benefit in relation to this tender is doing so fraudulently.

In the event of any such fraudulent communication, call, email, or solicitation, bidders are advised to immediately report the matter to the Tender Inviting Authority at the details mentioned below:

E-mail ids: [ccmanager@iimb.ac.in](mailto:ccmanager@iimb.ac.in); [tenders@iimb.ac.in](mailto:tenders@iimb.ac.in);

The TIA shall not be responsible for any loss or damage suffered by bidders due to dealings with unauthorised or fraudulent persons.

**Indian Institute of Management Bangalore**

## Table of Contents

Request for Proposal for the selection of Implementation of the IIMB Shield 2026 for the Indian Institute of Management Bangalore.....	1
DISCLAIMER.....	2
1. ABOUT IIMB: .....	5
2. ABOUT THE TENDER: .....	5
3. SCOPE OF WORK: .....	5
Technical Proposal: .....	5
3. COMMON DELIVERABLES (APPLICABLE TO ALL PHASES) .....	7
4. PHASE-1: IDENTITY, ENDPOINT & NETWORK SECURITY HARDENING .....	7
5. PHASE-2: DPDP COMPLIANCE & DATA GOVERNANCE ENABLEMENT .....	8
5.1 Deliverables.....	8
5.2 Acceptance Criteria .....	8
6. PHASE-3: ZERO TRUST SECURITY MATURITY ENHANCEMENT .....	8
6.1 Deliverables.....	8
6.2 Acceptance Criteria .....	8
7. PHASE COMPLETION & SIGN-OFF .....	9
8. MASTER COMPLIANCE & DELIVERY CHECKLIST .....	9
8.1 Pre-Engagement Checklist .....	9
8.2 Phase-1 Completion Checklist.....	9
8.3 Phase-2 Completion Checklist.....	9
8.4 Phase-3 Completion Checklist.....	9
Technical Implementation & Optimisation Matrix.....	9
1. Eligibility Criteria (Mandatory – Pass/Fail).....	14
1.1 Organisational Eligibility.....	14
1.2 Financial Eligibility.....	14
1.3 Experience & Track Record .....	14
1.4 Conflict of Interest & Independence.....	15
2. Technical & Commercial Selection Criteria.....	15
2.1 Evaluation Methodology.....	15
3. Technical Evaluation Scoring (Total: 100 Marks) .....	15
3.1 Technical & Solution Fit – 45 Marks.....	15
3.2 Experience & References – 25 Marks .....	15
3.3 Governance & Delivery Capability – 20 Marks .....	16
3.4 Certifications & Skills – 10 Marks.....	16
4. Qualification Threshold.....	16
5. Financial Evaluation (Post-Qualification).....	16
4. ELIGIBILITY CRITERIA:.....	16

5. Pre-bid Meeting:.....	18
6. EMD:.....	18
7. TENDER SCHEDULE: .....	19
8. BID VALIDITY PERIOD:.....	20
9. INSTRUCTIONS TO ONLINE BID SUBMISSION:.....	20
9.1. Registration: .....	20
9.2. Preparation of Bids: .....	21
9.3. Submission of Bids:.....	21
9.4. ASSISTANCE TO BIDDERS: .....	23
10.OPENING OF BIDS:.....	24
11.EVALUATION OF BIDS:.....	24
11.1. Technical Bid Evaluation:.....	24
11.2. Technical and Financial Bid Evaluation:.....	24
11.2(f) Presentation:.....	24
12.AMENDMENT/ CANCELLATION OF TENDER DOCUMENT:.....	25
13.AWARD OF CONTRACT AND COMMENCEMENT OF OPERATION:.....	25
13.1. Letter of Award (LoA): .....	25
13.2. Performance Security: .....	25
13.3. Signing of Contract: .....	26
13.4. Commencement of operations:.....	26
13.5. Period of the Contract:.....	26
14.GENERAL CONDITIONS OF CONTRACT .....	26
ANNEXURE I.....	30
ANNEXURE II.....	31
ANNEXURE III.....	32
ANNEXURE IV.....	33
ANNEXURE V.....	34
ANNEXURE VI.....	35
ANNEXURE VII.....	36
ANNEXURE VIII.....	37

## 1. ABOUT IIMB:

Indian Institute of Management Bangalore (IIMB) (hereinafter referred to as the “Institute”), an Educational Institute of National Importance, invites E- bids on a two-bid system for the selection of implementing IIMB Shield 2026 at the **Indian Institute of Management Bangalore**. The tender document can be downloaded from the Central Public Procurement Portal (<https://eprocure.gov.in/eprocure/app>). Submission of e-Bids will be made only through the e-Tender portal at <https://eprocure.gov.in/eprocure/app>. Bids will not be accepted in any other form.

## 2. ABOUT THE TENDER:

The IIMB Shield 2026 program is a one-year strategic cybersecurity and compliance engagement designed to:

- Achieve ISO/IEC 27001 certification readiness
- Achieve DPDP Act (India) compliance
- Strengthen IIMB’s Zero Trust Security (ZTS) maturity
- Reduce institutional cyber risk while leveraging existing investments in Microsoft, Cisco, and Sophos platforms

This engagement positions cybersecurity as an operational risk-reduction and compliance enablement initiative

## 3. SCOPE OF WORK:

### Technical Proposal:

1.1 The objective of this engagement is to provide **time-bound, outcome-oriented technical support** for:

- (a) ISO/IEC 27001 certification readiness,
  - (b) Digital Personal Data Protection (DPDP) Act, 2023 compliance enablement, and
  - (c) Zero Trust Security Maturity enhancement,
- under the programme titled “**IIMB Shield 2026**”.

1.2 This engagement shall focus **exclusively on technical implementation, integration, validation, knowledge transfer and stabilisation**, and shall **explicitly exclude vCISO or policy-only advisory services**.

1.3 The engagement shall be executed in **three (3) defined phases**, on a **milestone-based, fixed-price** model, maximising the Institute’s **existing security investments** and introducing external tooling **only where justified and approved** for maturity enhancement.

## In-Scope Platforms (Baseline):

### Current license details

- Microsoft M365 A3 security components (Entra ID P1(500), MFA, Conditional Access, Cloud App Discovery, Enterprise Mobility +Security A3, Intune for Education, Entra P2 license for Admin (1 nos), Defender email security, MS Purview foundations, Endpoint defender for BYOD along with dashboard for comprehensive integration, visibility and security control)
- Cisco Security Stack (ISE (with Premier lice), Cisco Secure client (with Apex lice) (2500No's)FTD/FMC/DNAC,& Meraki cloud)
- Sophos Endpoint (900 No's) & XDR -server (60 No's)(Sophos API's, Microsoft Office 365 Management Activity, Microsoft Office 365 Management Activity, Response Action Integrations)
- Vendor needs to check and configure all above features at central level and implement atleast 50 different users/stakeholders before handing over the SOPs and self service portal for the operational team to continue further and comeback in case of any issues faced during support period.

### ISO 27001:2022 Certification Readiness

#### Current Status and Scope Overview

IIM Bangalore has already initiated the implementation of an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. The current status of work is as follows:

- ISMS Policies and Procedures documentation has been completed to approximately 60–70%.
- Evidence collection and control implementation records have been completed to approximately 50%.
- Completion and finalization of all pending ISMS documentation to ensure 100% compliance with ISO/IEC 27001:2022 requirements.
- ISO 27001:2022 gap assessment against the current SoA. Walk through 87 applicable controls; reassess applicability of currently-Excluded controls; produce control-by-control gap register, evidence collection.
- Documentation gap inventory: which ISMS-required documents (policies, SOPs, registers) are missing or out of date.
- Review the existing/ Drafting of the ISMS policies and SOPs identified in the documentation gap inventory (information security policy, access control policy, acceptable use, incident response, supplier management, business continuity, etc.), then reviewed with the CISO Office
- ISO 27001:2022 certification path recommendation: timeline, internal audit readiness gates, Stage 1 / Stage 2
- Automation setup for ISO 27001:2022 evidence collection.

## 2.2 Maturity Extensions (Phase-3):

- Security Service Edge (SSE) capabilities such as CASB, ZTNA, Secure Web Gateway, and advanced / cross-platform DLP, SD-WAN, ARM, DWM, SOC/SIEM where required to meet Zero Trust maturity outcomes.

## 2.3 Out-of-Scope (Across All Phases):

- vCISO or long-term governance roles
- Legal interpretation of regulations
- Managed SOC or 24x7 operational services
- License procurement beyond explicitly approved recommendations

### 3. COMMON DELIVERABLES (APPLICABLE TO ALL PHASES)

#### 3.1 Project Governance & Management

- Project kick-off, delivery plan, RACI
- Weekly status reports and risk register
- Change and decision logs

#### 3.2 Knowledge Transfer & Capacity Building

- Structured knowledge transfer sessions
- “As-built” documentation and runbooks
- Operational handover sign-off

#### 3.3 Audit-Ready Evidence Enablement

- Tool-generated evidence artefacts
- Reproducible logs, reports, and screenshots
- Control-to-objective mapping documentation

#### 3.4 Post-Implementation Stabilisation

- Hypercare and stabilisation support per phase
  - **ISO certification readiness -compliance (45 days + 45 days support) –**  
The vendor shall complete all ISO-related documentation, evidence collection, and automation of compliance requirements within forty-five (45) calendar days from the project commencement date. Following the Pre- ISO audit, the vendor shall provide forty-five (45) calendar days of post-audit support, including remediation assistance and clarifications, as required.
  - **DPDP compliance (45 days + 45 days support)**  
The vendor shall complete all required documentation and evidence collection for DPDP compliance within forty-five (45) calendar days. Upon completion of documentation and applicable tool automation, the vendor shall provide forty-five (45) calendar days of post-implementation support to address observations, updates, and compliance-related queries.
  - **Zero Trust security maturity enhancement (90 days + 95 days support).**  
The vendor shall design, suggest , justify ,deploy, and test all required tools, infrastructure, and controls to further enhance Zero Trust security maturity within ninety (90) calendar days. Upon successful implementation, the vendor shall provide ninety-five (95) calendar days of post-implementation support, including monitoring support, issue resolution, and fine-tuning of deployed controls.
- Closure sign-off post stabilization
  - Closer report should have all configuration details, with screenshots of the tools used details

### 4. PHASE-1: IDENTITY, ENDPOINT & NETWORK SECURITY HARDENING

#### 4.1 Deliverables

- 4.1.1 Phase-1 Baseline Security Assessment & Hardening Roadmap
- 4.1.2 Identity Security Hardening and Risk-Based Access Controls
- 4.1.3 Endpoint Hardening and Detection Readiness

- 4.1.4 Network Admission Control (NAC) and Segmentation Baseline
- 4.1.5 Cross-Stack Integration Enablement (Identity–Endpoint–Network)
- 4.1.6 Phase-1 Security Evidence Pack
- 4.1.7 Phase-1 Knowledge Transfer & Runbooks, policy documents

#### **4.2 Acceptance Criteria**

- Identity, endpoint, and network security controls are implemented and enforced for the agreed pilot and rollout scope
- Cross-tool integrations are functional and validated
- No unresolved high-severity operational issues attributable to Phase-1 changes
- Evidence pack accepted by IIMB IT Security stakeholders

### **5. PHASE-2: DPDP COMPLIANCE & DATA GOVERNANCE ENABLEMENT**

#### **5.1 Deliverables**

- 5.1.1 DPDP Readiness Assessment and Gap Register
- 5.1.2 Personal Data Inventory and Data Flow Mapping
- 5.1.3 Consent, Erasure, and Reporting Architecture Enablement
- 5.1.4 Fine-Tuning and Integration of Existing Tools for DPDP Controls
- 5.1.5 Automated / Real-Time Evidence Collection Approach
- 5.1.6 DPDP Documentation Pack for Stakeholders
- 5.1.7 Audit Support & DPDP Compliance Reporting Artefacts
- 5.1.8 Phase-2 Knowledge Transfer & Runbooks

#### **5.2 Acceptance Criteria**

- DPDP gaps identified and addressed through technical controls
- Personal data flows are documented and validated by data owners
- Data Principal Rights workflows demonstrably supported
- DPDP evidence pack auditable and reproducible from systems

### **6. PHASE-3: ZERO TRUST SECURITY MATURITY ENHANCEMENT**

#### **6.1 Deliverables**

- 6.1.1 Zero Trust Maturity Gap Assessment & Target Architecture
- 6.1.2 External Tool / Licence Recommendation & Justification Dossier
- 6.1.3 Implementation and Integration of Approved External Platforms
- 6.1.4 Zero Trust Network Access (ZTNA) Pilot for Defined Applications
- 6.1.5 Cloud & SaaS Governance Controls (CASB, where applicable)
- 6.1.6 Advanced / Cross-Platform Data Protection Controls
- 6.1.7 Validation & Table-Top Exercises for Zero Trust Scenarios
- 6.1.8 Phase-3 Evidence Pack, As-Built Architecture & Handover

#### **6.2 Acceptance Criteria**

- Target Zero Trust architecture approved and operational
- Approved external controls implemented and integrated with baseline stack
- ZTNA enforced for agreed applications with verified access logs
- Validation exercises completed with documented outcomes

- Operations team enabled to independently manage deployed controls

## 7. PHASE COMPLETION & SIGN-OFF

### 7.1 Each phase shall be deemed complete upon:

- Delivery of all phase-specific deliverables,
- Fulfilment of acceptance criteria, and
- Formal sign-off by authorised IIMB representatives
  - The vendor shall secure approval from the respective IIMB domain stakeholders, followed by final sign-off from the Campus Computer Manager.

**7.2 Phase sign-off shall trigger milestone-based commercial payments as per the contract.**

## 8. MASTER COMPLIANCE & DELIVERY CHECKLIST

### 8.1 Pre-Engagement Checklist

- Administrative access provisioned
- Asset and application inventory shared
- Change windows and blackout periods confirmed

### 8.2 Phase-1 Completion Checklist

- Identity, endpoint, network hardening live
- Integrations validated
- Evidence pack & KT completed

### 8.3 Phase-2 Completion Checklist

- DPDP readiness and data flows approved
- Consent / erase workflows demonstrated
- DPDP evidence & documentation delivered

### 8.4 Phase-3 Completion Checklist

- Zero Trust target architecture approved
- External tools (if approved) operational
- ZTNA pilot completed
- Validation exercises concluded
- Final handover sign-off obtained

## Technical Implementation & Optimisation Matrix

### Phase 1 A: Identity & Endpoint Hardening (The "Front Door")

Stream	Technical Check Item & Implementation	Success Metric / Deliverable
<b>ISO 27001:2022 Certification Readiness</b>	<p><b>ISO 27001:2022 gap assessment</b> across SoA, 87 controls, exclusions review, gap register, and evidence identification.</p> <p><b>ISMS documentation gap analysis</b>, identifying missing or outdated policies, SOPs, and risk register.</p> <p><b>Drafting and review of ISMS policies/SOPs</b>, validated with the CISO &amp; Team</p> <p><b>Certification roadmap recommendation</b> covering timeline, audit readiness, and Stage 1 / Stage 2 audits</p> <p>Awareness training for the IIMB Community.</p> <p>Select, deploy the Automation setup for ISO 27001:2022 evidence collection and status report generation (No procurement or supply)</p>	<p>Readiness for ISO 27001:2022 Certification in line with Automation setup for ISO 27001:2022 evidence collection and status report generation.</p>
<b>Entra ID / M365</b>	<p>Enforce MFA (Conditional Access) &amp; Block Legacy Auth; Configure Named Locations (Campus IPs).</p>	<p>100% MFA adoption; 0 Legacy Auth sign-ins in logs.</p>
<b>Intune for Education</b>	<p>Deploy MDM/MAM; Define Compliance Policies (Disk Encryption, OS Build, Antivirus status).</p>	<p>100% managed device enrolment; Compliance-gated access.</p>
<b>Sophos XDR/Ms Defender EDR</b>	<p>Integration of Sophos XDR (Data lake) with ISE /M365 / Microsoft - Graph Security API V2/Meraki/FMC for audit logs and event correlation through Sophos XDR-based threat alert, analysis and hunting.</p>	<p>Agent heartbeat on all assets, IT Components &amp; tools; Automated isolation playbooks active.</p>
<b>Data</b>	<p>Activate Sophos DLP, Defender DLP, Purview DLP (Exchange/SharePoint/OneDrive); Publish</p>	<p>DLP alerts active; User training on manual</p>

<b>Protection</b>	Sensitivity Labels.	labelling completion.
-------------------	---------------------	-----------------------

### Phase 1 B: Network Fabric & Zero Trust Access (The "Internal Guard")

Stream	Technical Check Item & Implementation	Success Metric / Deliverable
<b>Cisco ISE</b>	Enforce 802.1X on wired/wireless; Active Device Profiling; Posture Assessment enforcement. Activate Cisco Secure Client Apex modules: ISE Posture (off-network compliance),	Zero unauthenticated network access; Posture-based VLAN assignment.
<b>Cisco /ISE/ FTD/FMC</b>	Define Security Zones (Academic, Admin, IoT, Guest); Enforce Inter-zone Least Privilege; SSL/TLS Inspections, assignment, session control, access control, posture checking, trustSec, and policy control in FTD/ FMC.	Validated micro-segmentation; Encrypted traffic visibility active.
<b>Integration</b>	Feed Sophos posture into ISE via pxGrid; Integrate Entra ID signals into ISE NAC decisions.	Identity-Aware NAC: Network access revoked if Sophos detects a threat.
<b>Access Mgmt</b>	Establish Guest/Contractor portals with time-limited workflows.	Automated guest credential expiration; Logged contractor activity.

### Phase 2: DPDP Compliance & Data Governance

Stream	Technical Check Item & Implementation	Success Metric /
--------	---------------------------------------	------------------

		<b>Deliverable</b>
<b>Data Discovery</b>	Implement automated data discovery to map PII/Sensitive data across AWS, Azure, and On-Prem.	Comprehensive Data Map and Data Flow Diagrams.
<b>Compliance</b>	Align Purview Audit Log retention with DPDP/ISO requirements; Consent Architecture review.	Audit logs retained for 1 year+; "Right to Erasure" workflow documented.
<b>Governance</b>	Develop Data Classification Framework (Policy); Assign Data Stewards.	Framework published; Owners assigned to all 300+ critical assets.

### Phase 3 Advanced Maturity & Performance Optimization

<b>Stream</b>	<b>Technical Check Item &amp; Implementation</b>	<b>Success Metric / Deliverable</b>
<b>Capability</b>	Select, deploy ZTNA for per-app access (replacing VPN), if required. (No procurement or supply)	Critical apps hidden from public internet; Risk-based "Impossible Travel" blocks.
<b>Monitoring</b>	Select and enable Dark Web Monitoring for domains; Establish SOC Operations (SIEM aggregation) if found insufficient. (No procurement or supply)	24/7 Monitoring active; Leaked credential remediation < 1hr.
<b>Performance</b>	Select and deploy Application Performance monitoring tool if required. (No procurement or supply)	Bottlenecks identified/removed;

	supply)	Latency baseline documented.
<b>Validation</b>	Annual 3rd Party VAPT report validation; Annual Web Security Scoring report validation.	Remediation report signed off; Public-facing site score > A.
<b>Enchantment of Security - M365 A5</b>	Upgrade to M365 A5 Faculty (preferred) or add Entra ID P2 standalone. A5 unlocks Teams DLP, Endpoint DLP, MDO P2, Insider Risk, eDiscovery Premium, Advanced Audit. (No procurement or supply)	Risk-based Conditional Access active, PIM deployed for admin roles, Identity Protection is in operation.
<b>PAM</b>	Select, deploy PAM for on-premises and infrastructure admin accounts (accounts). Integrate with Entra ID P2 PIM for cloud admin scope. (No procurement or supply)	All admin accounts vaulted; sessions recorded; rotation automated; and report generation.
<b>DLP Policy enhancement</b>	DLP deployment (included in A5 or third-party). Extend Teams DLP scope. Enable Insider Risk Management (No procurement or supply)	DLP rules active; Insider Risk policies are operational, alert configuration & compliance automation reports configuration & as per the DPDP Act, 2023.
<b>CSPM</b>	Select, deploy Cloud Security Posture Management (CSPM) for AWS and Azure. Optional CWPP for runtime workload protection (No procurement or supply)	Detects over-privileged IAM roles, unused service accounts, Detects open ports, public endpoints, flat networks, ensures encryption,

		Continuous posture scanning & risk scoring Auto-remediation of policy violations, Cloud findings are ingested into the SIEM.
<b>IoT segmentation</b>	Strengthen IoT segmentation via expanded ISE profiling and FTD zone policies.	All IoT devices profiled; isolated in dedicated zones; policy enforcement verified.
<b>DNS-layer security</b>	Select, deploy DNS-layer security for off-network and on-network protection. Pairs with Secure Client roaming module. (No procurement or supply)	DNS-layer threat blocking, no credential theft, Protects users on-network, remote, cloud, and roaming devices. Low latency, high coverage  Alert sent configuration.

## 1. Eligibility Criteria (Mandatory – Pass/Fail)

Only bidders meeting **all** the following eligibility conditions shall be considered for technical evaluation. Non-compliance with **any one criterion** will result in outright disqualification.

### 1.1 Organisational Eligibility

1. The bidder must be a company / LLP / partnership /proprietorship legally registered in India and operational at the time of bid submission.
2. The bidder must have been engaged in **cybersecurity consulting and implementation services** for a **minimum of 5 (five) continuous years** as on the bid submission date.
3. The bidder must have an operational presence in India with identified technical and delivery resources available for **on-site and remote delivery**.

### 1.2 Financial Eligibility

4. The bidder must have achieved a **minimum average annual turnover** ( 50 lacs) during the last **three financial years** from cybersecurity, IT security, or information security services. Audited financial statements or CA-Certified turnover certificate must be submitted.
5. The bidder should not be insolvent, blacklisted, or under litigation that may materially affect delivery of this engagement. Self-declaration to be provided.

### 1.3 Experience & Track Record

6. The bidder must have executed **at least three (3) cybersecurity transformation/implementation projects** covering a **minimum 70% of this RFP scope**, involving:
  - Zero Trust security implementation
  - Identity, Endpoint, Network, and cloud security components integration
  - Data Protection domains
  - ISO 27001:2022 audit readiness
7. At least **one engagement** must be in a **large enterprise/university / public-sector / regulated institution** with:
  - $\geq 2,000$  users **OR**
  - Multi-campus or hybrid IT infrastructure
 Completion certificates with project scope and timelines must be submitted.
8. The bidder must demonstrate experience in **ISO 27001:2022 /IEC 27001 implementation or readiness** for a **minimum two (2) clients**, supported by sample audit or readiness reports.
9. The bidder should have experience in **data protection/privacy compliance Programmes** (DPDP Act, GDPR or equivalent) for a **minimum three (3) clients**, with sample artefacts.

### 1.4 Conflict of Interest & Independence

10. The bidder must **not** be a reseller-led or license-bundled bidder but have sufficient skills to assess and mitigate the security loopholes.  
vCISO services, license resale, or managed SOC outsourcing must not be bundled as part of this bid.

## 2. Technical & Commercial Selection Criteria

### 2.1 Evaluation Methodology

- Bids will be evaluated under a **two-stage process**:
  1. **Stage 1 – Eligibility (Pass/Fail)**
  2. **Stage 2 – Technical Evaluation (100 Marks)**
- **Only bidders scoring  $\geq 70$  marks out of 100 in Technical Evaluation shall qualify for Financial Bid opening.**

## 3. Technical Evaluation Scoring (Total: 100 Marks)

### 3.1 Technical & Solution Fit – 45 Marks

Sub-Criteria	Max Marks
Zero Trust architecture covering Identity, Device, Network and Data layers	10
Integration design across Entra ID / AD / SSO, Cisco ISE, XDR/EDR, Firewall, Proxy, SIEM/SOC, Cloud (Azure/AWS)	10
ISO 27001 Annex-A control mapping with technical evidence	10
DPDP Act control mapping (Purpose Limitation, Consent, Retention, Erasure, Data Transfers)	10
Evidence automation, audit-ready artefacts & control validation methodology	5
<b>Total</b>	<b>45</b>

### 3.2 Experience & References – 25 Marks

Sub-Criteria	Max Marks
Similar Zero Trust / Cybersecurity transformation projects completed	10
Higher-education / public-sector / regulated-sector engagements	8

ISO 27001 & DPDP references with sample reports	7
<b>Total</b>	<b>25</b>

### 3.3 Governance & Delivery Capability – 20 Marks

Sub-Criteria	Max Marks
Project governance model, RACI, escalation, reporting structure , presentation & documentation neatness.	8
Quality of delivery methodology (phased approach, milestones, KT, stabilisation)	7
Availability of named key resources (PM, Security Architect, Compliance SME)	5
<b>Total</b>	<b>20</b>

### 3.4 Certifications & Skills – 10 Marks

Certification / Capability	Max Marks
ISO/IEC 27001 Lead Auditor / ISMS Certified resources	3
Microsoft Certified: Cybersecurity Architect / Azure Security Engineer	3
Network & Endpoint security skills (Cisco CCNP Security, Sophos, equivalent)	2
Privacy certification (CDPP / DSCI / DPDP-specific)	2
<b>Total</b>	<b>10</b>

## 4. Qualification Threshold

- **Minimum Technical Qualification Score: 70 / 100**
- Only bidders meeting:
  - **100% eligibility compliance**, and
  - **≥ 70 technical marks**
 will be considered **Technically Qualified**, and their **Financial Bids shall be opened**.

## 5. Financial Evaluation (Post-Qualification)

- Financial bids will be evaluated only for technically qualified bidders.
- Final L1 determination shall be as per IIMB procurement norms and tender conditions.

## 4. ELIGIBILITY CRITERIA:

All the Bidders must fulfil the following eligibility criteria and submit the scanned documents and the declarations in support of their claim along with the Technical Bid. The Technical Bids not meeting the Eligibility Criteria stated below and not accompanied with the requisite documents as sought below shall be treated as incomplete and will be rejected.

Sl.No	Qualifying Criteria	Supporting Documents
-------	---------------------	----------------------

a)	The nature of the organisation should be registered under the applicable acts in India.	Copies of company establishment/ company license.
b)	The bidder should be a firm registered and operating in India for at least 5 years, with a focus on cybersecurity consulting and implementation services.	Documents supporting the bidder status as a cybersecurity & ISO 27001:2022 ISOdocumentation-based company to be submitted
c)	The bidder's annual turnover in each of the previous three financial years (2022- 23, 2023 24 and 2024- 25) ₹ 50 lacs. This turnover should be that of the bidder alone, not that of the group the bidder belongs to.	Documents supporting the turnover, turnover certificate certified by CA and balance sheet to be submitted.
d)	The bidder should have successfully executed at least five similar assignments of cybersecurity consulting and implementation services conducted post 31 March 2025.	Documents supporting the Experience such as work order, work completion and invoices to be submitted.
e)	The bidder must give detailed documents for Technical Proposal along with the architecture diagram.	Write up with requisite documents supporting are to be submitted .
f)	The bidding entity should have Permanent Account Number(PAN) and GST	A copy of the PAN (Permanent Account Number) and GST
g)	The bidding firm should be neither blacklisted by any Government Dept., nor is any criminal case registered / pending against the firm or its owner / partners anywhere in India.	A duly completed certificate to this effect is to be submitted as per Annexure-III.

h)	Annexures	Annexures I, II, IV, V to VIII duly filled, signed and with company seal

Note: Exemption for only EMD will be provided to the MSE and startups. No Exemption or relaxation for Prior turnover and prior experience will be provided as the services are related to conducting an All-India examination with its own complexities.

## 5. Pre-bid Meeting:

Pre-bid meeting will be held on May 18<sup>th</sup>, 2026, at 11:00 am online through Zoom platform to address the queries of the bidders regarding the Tender. Interested bidders may send their queries on or before May 15<sup>th</sup>, 2026 by 15:00 Hrs. to the email id [ccmanager@iimb.ac.in](mailto:ccmanager@iimb.ac.in). The prospective bidders interested in participating in the Prebid meeting must send the email IDs to which the meeting link has to be shared to the mail id [ccmanager@iimb.ac.in](mailto:ccmanager@iimb.ac.in). The replies to the queries will be uploaded on the CPP Portal / IIMB Website.

## 6. EMD:

Interested Bidders are requested to pay the EMD for an amount of Rs 50,000/- (Rupees fifty thousand Only) should be submitted through NEFT, RTGS or Bank Guarantee in favor of Indian Institute of Management Bangalore.

### **Bank details for NEFT/RTGS transfer to IIMB.**

Bank Name : HDFC Bank Ltd  
Bank Street Address : J.P. NAGAR BRANCH, BANGALORE  
Branch Code : 0133  
IFSC CODE : HDFC0000133  
Customer HDFC Bank a/c name : Indian Institute of Management  
Customer HDFC Bank a/c number : 01331450000019

Copy of the UTR details for NEFT/RTGS transfer should be enclosed with the technical bid.

The scanned copy of the Bank Guarantee should be uploaded with the technical bid and the original must be delivered to the address below on or before the submission date; failing to do so may result in rejection of the bid.

Campus Computer Manager

Computer Center

Indian Institute of Management Bangalore

Bannerghatta Road, Bangalore-560076

i) **Micro and Small Enterprises (MSEs) only** as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) are exempted from EMD. However, they have to enclose valid UDYAM Registration Certificate for relevant category along with the Technical Bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy.

ii) The bidders who seek exemption from EMD as per clause no. 6(i) above, if they withdraw or modify their bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for the period of three years or as decided by the competent authority from being eligible to submit bids for contracts with the entity that invited the bids.

iii) EMD of unsuccessful bidders will be returned within 30 days of finalization of the tender. EMD of the successful bidder will be returned only after receipt of Performance Security.

iv) The amount of EMD (if any) is liable to be forfeited if the tenderer withdraws from the offer after submission of the tender or after the acceptance of the offer fails to enter a contract.

v) No interest will be paid on EMD.

## 7. TENDER SCHEDULE:

<b>Publish Date</b>	12.05.2026 11:30 Hrs	<b>Bid Opening Date</b>	27.05.2026 14:30 Hrs
<b>Document Download Start Date</b>	12.05.2026 12:00 Hrs	<b>Document Download End Date</b>	26.05.2026 12:00 Hrs
<b>Pre– Bid Meeting Date</b>	18.05.2026 11:00Hrs		
<b>Bid Submission Start Date</b>	12.05.2026 12:00 Hrs	<b>Bid Submission End Date &amp; time</b>	26.05.2026 14:00 Hrs

Note:

- i. If the bid opening date is declared an Institute holiday, the bids will be opened on the next working day.
- ii. IIMB may at its discretion extend/ change the schedule of any activity and intimate the prospective bidders by notifications through CPP Portal/IIMB Website
- iii. IIMB reserves the rights to accept or reject any bids or accept all bids either in part or in full or to split the order, or to annul the bidding process without assigning any reasons thereof.

## 8. BID VALIDITY PERIOD:

- The bid must be valid for 120 days from the date of opening of Technical Bids. A bid valid for a shorter period shall be rejected, being non-responsive. In exceptional circumstances, IIMB may request the bidders for the extension of the validity period.
- The bidders shall not be entitled during the said period, to revoke or cancel their tenders or to change the tenders given or any term thereof. In case of bidders revoking or canceling their bids or varying any terms in regard thereof, the earnest money (if any) deposited by bidder with their offers, will be forfeited and the bidder may be debarred / blacklisted as per IIMB/Govt of India Rules.

## 9. INSTRUCTIONS TO ONLINE BID SUBMISSION:

The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, preparing their bids in accordance with the requirements and submitting their bids online on the CPP Portal. More information was useful for submitting online bids on the CPP Portal may be obtained at: <https://eprocure.gov.in/eprocure/app>.

### 9.1. Registration:

- a. Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (URL: <https://eprocure.gov.in/eprocure/app>) by clicking on the link “Online bidder Enrollment” on the CPP Portal which is free of charge.
- b. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.
- c. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal. Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / nCode / eMudhra etc.), with their profile.
- d. Only one valid DSC should be registered by a bidder. Please note that the bidders a responsible to ensure that they do not lend their DSC's to others which may lead to misuse.
- e. Bidder then logs in to the site through the secured log-in by entering their user ID /password and the password of the DSC / e-Token.

## 9.2. Preparation of Bids:

- a. Bidder should consider any corrigendum published on the tender document before submitting their bids.
- b. Bidder to go through the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the documents that need to be submitted. Any deviations from these may lead to rejection of the bid.
- c. Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF/JPG formats. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.
- d. To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Space" or "Other Important Documents" area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

Note: My Documents space is only a repository given to the Bidders to ease the uploading process. If Bidder has uploaded his Documents in My Documents space, this does not automatically ensure these Documents being part of Technical Bid.

## 9.3. Submission of Bids:

1. **Language of bid:** Bids and all related documents as well as all subsequent correspondence between the Bidder and IIMB shall be in English language. Supporting documents and printed literature furnished by the Bidder may be in another language provided they are accompanied by an accurate translation of the relevant passages in English, in which case for purpose of interpretation of the bid, the translation in English shall prevail.
2. Bidder should log into the site well in advance for bid submission so that they can upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
3. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document.
4. Bidders are requested to note that they should necessarily submit their financial bids in the BoQ format provided and no other format is

acceptable. If the price bid has been given as a standard BoQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BoQ file, open it and complete the colored (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BoQ file is found to be modified by the bidder, the bid will be rejected.

5. The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this during bid submission.
6. All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. The confidentiality of the bids is maintained using the secured Socket Layer 128-bit encryption technology. Data storage encryption of sensitive fields is done. Any bid document that is uploaded to the server is subjected to symmetric encryption using a system generated symmetric key. Further this key is subjected to asymmetric encryption using buyers/bid opener's public keys. Overall, the uploaded tender documents become readable only after the tender opening by the authorized bid openers.
7. Upon the successful and timely submission of bids (i.e. after Clicking "Freeze Bid Submission" in the portal), the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
8. The bid summary has to be printed and kept as an acknowledgment of the submission of the bid.

9. The bid should be submitted in two Bids

**A. Technical Bid:**

(a) EMD: Copy of the UTR details for online transfer to IIMB or Copy of the Bank guarantee as per Annexure IV Or Udyam Registration Certificate for EMD exemption

(b) Copies of the documents supporting Eligibility Criteria 4 a. to 4.l

(c) Annexures I-III and V-VIII duly filled and signed.

**B. Financial Bid:**

Bidders are requested to note that they should submit their financial bid in the BoQ format provided and no other format is acceptable.

A Screenshot of the BoQ is as below

[Validate](#) [Print](#) [Help](#) [Item Rate BoQ](#)

Tender Inviting Authority: Campus Computer Manager

Name of Work: Request for Proposal for selection of Service Provider to cybersecurity for Indian Institute of Management Bangalore Contract No: IIMB/IT/2025-26/01

Name of the Bidder/ Bidding Firm / Company:						
PRICE SCHEDULE (This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)						
Sl. No.	Item Description	Per	Units	BASIC RATE In Figures To be entered by the Bidder Rs. P	TOTAL AMOUNT Without Taxes	TOTAL AMOUNT In Words
1	Configuration and ISO certification readiness (45 days + 45 days support)					
2	DPDP compliance (45 days + 45 days support)	1.000	Nos		0.00	INR Zero Only
3	Zero Trust security maturity enhancement (90 days + 95 days support)	1.000	Nos		0.00	INR Zero Only
Total in Figures					0.00	INR Zero Only
Quoted Rate in Words					INR Zero Only	

**This is for reference only and not to be filled and submitted along with the Technical Bid.**

**Note for Financial bid and the Price quoted by the Bidders:**

- Bidders must quote in Indian Rupees only.
- The Prices quoted shall be kept firm throughout the duration of contract of this work and no price escalation shall be entertained.
- Price schedule should include all required services of the modules as per the tender.

**9.4. ASSISTANCE TO BIDDERS:**

- Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the email id [cmanager@iimb.ac.in](mailto:cmanager@iimb.ac.in) on or before **15<sup>th</sup> 05 2026** by **15:00 PM**
- Any queries relating to the process of online bid submission or queries relating to CPP Portal, in general, may be directed to the

24x7 CPP Portal Helpdesk numbers.

## 10. OPENING OF BIDS:

- Technical Bids will be opened on **27.05.2026**. At 14:30 Hrs
- Financial Bids of the eligible bidders will be opened on a later date. The date and time for opening of Financial Bids will be intimated through CPP Portal.

## 11. EVALUATION OF BIDS:

### 11.1. Technical Bid Evaluation:

Bidders should comply with scope of work and eligibility criteria; no deviations are acceptable. The bidder is to complete the same in all respect and submit accordingly. The bids which meet all the eligibility criteria and submitted all the documents for the same will be qualified on eligibility criteria and eligible for further evaluation. Bids not meeting the eligibility criteria will be rejected and not considered for further evaluation. If any information/documents provided in the technical bids are proved to be false, the technical bid will be rejected.

### 11.2. Technical and Financial Bid Evaluation:

IIMB will evaluate the proposals based on several criteria. Each criterion will be assigned a specific score. The overall evaluation of a proposal will be determined by the **total score obtained across all the criteria**.

The details of the evaluation criteria along with the **maximum score allocated to each criterion** are provided below.

#### 11.2(f) Presentation:

The presentation should not be more than 10 -15 PPT slides. PPT needs to attached along with other tender documents, and the presentation should cover all the ISO/IEC 27001 certification readiness scope, DPDP Act, 2023 compliance mitigation approach & Zero Trust Security Maturity enhancement in detail, with the outcome of each scope.

The presentation can be asked in person in next 4-5 days from the submission date 25<sup>th</sup> May'26 and will be for 25min, followed by 15 min for Q & A. The IIMB technical team will evaluate each bidder's presentation and assign marks.

Note: The purchase preference will be given to MSEs having valid Udhya Registration and whose credentials are validated online through Udhya Registration Portal as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 12.02.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. In respect of bid for Services, the bidder must be Service provider of the offered service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service.

## **12. AMENDMENT/ CANCELLATION OF TENDER DOCUMENT:**

At any time prior to the deadline for submission of proposals, Institute may for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder modify the Tender Document by issuing an addendum/corrigendum. Any Addendum/corrigendum thus issued shall become a part of the Tender Document and will also be posted on the website of the Institute. To provide reasonable time to the prospective Bidders to take an addendum into account while preparing their proposals, the deadline for submission of proposals may be extended, at the discretion of IIMB, if required.

IIMB has the right to cancel this tender at any point of time without assigning any reasons.

## **13. AWARD OF CONTRACT AND COMMENCEMENT OF OPERATION:**

The IIMB will award the Contract to the successful service provider as determined above, provided further that the Bidder has been determined to be qualified to satisfactorily perform the Contract.

Before issuing a Letter of Award (LoA) to the successful service provider, IIMB may, at its discretion, ask Bidder to submit for verification the originals of all such documents whose scanned copies were submitted online along with the technical bid.

### **13.1. Letter of Award (LoA):**

The Bidder, whose bid has been accepted and documents verified (at the discretion of IIMB), shall be issued a Letter of Award by IIMB.

### **13.2. Performance Security:**

A Performance security(PS) at 5% on the contract value in the

form of Bank Guarantee drawn from any nationalized bank or in the form of online bank transfer to IIMB shall be provided by the Bidder within 14 days from the date of issue of letter of award. The PS shall be valid for the contract period and additional three months.

The PS shall be released after the completion of the work pursuant to this Contract based on the "Completion Certificate" issued by IIMB stating that the Bidder has completed the work in all respects, satisfactorily. The PBG, however, shall be released only after the expiry of the contract period, and after clearance of the final bill based on "**No Claim Certificate**" from the Bidder.

In case where the Contract has been rescinded, the PS will be forfeited, and the Bank Guarantee shall be encashed and the balance work shall be completed independently by IIMB at the risk and cost of the Original successful Bidder.

In case the contract being determined as terminated or rescinded under provision of the contract, the PS shall be forfeited in full.

**Within 14 days of receipt of the Letter of Award, Performance security shall be submitted by the contractor to IIMB.**

### 13.3. Signing of Contract:

Within seven working days of receiving performance security, the successful bidder should execute a contract with IIMB. A non-disclosure agreement also needs to be entered into.

### 13.4. Commencement of operations:

The successful bidder shall commence the service within 7 days from the date of LOA.

### 13.5. Period of the Contract:

The contract is for a period of 12 months and the same would be from the date of commencement of service. The contract Price shall be as per the Quote for each year.

## 14. GENERAL CONDITIONS OF CONTRACT

- i) **Default:** In the event the Bidder contravenes any of the provisions of the Contract or neglects to carry out his obligations of the Contract, IIMB may give notice in writing thereof requiring the Bidder to remedy the breach within seven days, or within such period as IIMB may agree to be reasonable

and in the event of the Bidder failing to do so, IIMB will be at liberty to procure the services from third party vendors or have the work which the Bidder has neglected to do, carried out by a third party at the Bidder's cost and risk. In such an event IIMB shall have the right to terminate the Contract.

**ii) Intellectual Property Rights (IPR)**

- a. The Bidder undertakes not to, in any manner, claim all or any part of the IPR or commercially exploit all or any of the proprietary rights generated and developed by IIMB as vested whether trademarked, copyrighted or not.
- b. The Bidder acknowledges that all IPR relating to the entire content of the existing IIMB website, and all the output relating to the service belongs to and vests exclusively with IIMB and under no circumstances whatsoever the Bidder shall claim all or any rights proprietary or otherwise over all or any portion of the IPR belonging to IIMB.
- c. Work made for hire: The Bidder expressly acknowledges that the material contributed by it hereunder, and its services hereunder, are being specially ordered and commissioned by IIMB for use in connection with the service. The work contributed by the Bidder hereunder shall be considered a "work made for hire" as defined by the copyright laws. IIMB shall be the sole and exclusive owner and copyright proprietor of all rights and title in and to the results and proceeds of the Bidder's services hereunder in whatever stage of completion. If for any reason the results and proceeds of the Bidder's services hereunder are determined at any time not to be a "work made for hire", the Bidder hereby agrees to irrevocably transfer and assign to IIMB all right, title and interest therein, including all copyrights, as well as all renewals and extensions thereto.

**iii) Data Security:** The Bidder shall use inputs provided by IIMB solely for performing its obligations under this Contract, and will not, at any time, transfer, save, download, print, disclose, or in any other way use the inputs other than as directly required for the provision of the services under this Contract or as directed by IIMB in writing.

**iv) Access transfer:** The Bidder shall share complete knowledge transfer of user ids, passwords, and other access details etc. to IIMB at any time.

**v) Confidentiality:** Both the Parties hereby undertake that under no circumstances whatsoever they shall disclose any of the Terms of this Contract and all or any Confidential Information belonging to the other party like financial plans, business plans, and others, declared confidential to which they might have access during the association with one another in terms of this Contract, except to the extent that is already in public knowledge/ domain. The Confidential Information as hereinabove detailed shall not be disclosed during the subsistence of this Contract and thereafter

for a period of five years from the date of termination of this Contract for whatever reason. The successful bidder is required to enter into a non-disclosure agreement.

- vi) Indemnity:** Either Party (Indemnifying Party) shall indemnify, defend and hold harmless the other Party (Indemnified Party), its directors, officers and employees from and against any and all claims, demands, liabilities, and reasonable attorney's fees but only in proportion to and to the extent such claims, liabilities, and attorney's fees arise from any errors and any act/commission/omission on part of the Indemnifying Party or in connection with any work, authority or jurisdiction delegated to the Indemnifying Party under this Contract.
- vii) Arbitration:** Any dispute arising under the terms of this Contract which cannot be resolved by the Parties shall be referred to arbitration as mutually agreed by the parties, in writing. The said Arbitration shall act under the provisions of the Arbitration and Conciliation Act, 1996 or any statutory modifications or re-enactment thereof or any rules made thereof. The arbitration shall take place in Bangalore, India. Proceedings shall be conducted, and documentation presented in English. It shall further be agreed that, the decision of the arbitration shall be final and binding on both the Parties.
- viii) Jurisdiction:** This Contract shall be governed and construed in accordance with the Indian Laws and subject to the exclusive jurisdiction of competent courts at Bangalore, India.
- ix) Termination:**
- a. Termination for convenience: Either Party can terminate the Contract for convenience, by giving at least 120 days prior written termination notice to the other Party.
  - b. Termination due to Breach: In the event the successful bidder materially breaches the Contract, IIMB may, without prejudice to its other rights and remedies, terminate the Contract by giving prior written notice of thirty (30) days, provided that the breach remains uncured at the end of such notice period.
  - c. Termination for Insolvency: IIMB may terminate the Contract Agreement upon written notice to the successful bidder in the event the said bidder (i) seeks reorganization or release under applicable law, (ii) seeks the appointment of a trustee, receiver or custodian, (iii) becomes the subject of a proceeding seeking the liquidation, winding-up, dissolution, reorganization or the like of the said bidder, and such proceeding is not dismissed within sixty (60) days of the commencement thereof, (iv) makes an assignment for the benefit of creditors, or (v) has a substantial part of the said bidder's property become subject to any levy, seizure, assignment, application or sale for or by any creditor or government agency.

d. Effect of termination: In the event of termination of the Contract, the successful bidder agree to promptly deliver all the deliverables applicable to the fullest extent conceived, created or developed prior to the date of termination.

Further, upon termination of the Contract, (i) the successful bidder shall cease to provide the Services (ii) IIMB's only liability shall be to pay the fees for the Services completed to the satisfaction of IIMB.

**x) Assignment:** The Bidder shall not transfer, assign or sublet the Contract or any part thereof without the prior written consent of IIMB. Any permitted transfer/assignment or subletting shall not relieve the Bidder of any of his obligations which might have arisen before such permission was given.

**xi) Notice:** All notices, including notice of address change, required to be sent hereunder shall be in writing and shall be deemed to have been delivered when mailed by first class mail or reputed courier service return receipt requested, to the address stated in the first page of the SLA. Electronic communications are admissible provided these are sent with delivery confirmation receipt and followed by physical copy mailed as set forth above.

**xii) Force Majeure:** No Party shall be in default under this Contract by reason of its failure or delay in the performance of its obligation, if such failure or delay is caused by acts of God, Government Laws and Regulations, Strikes/lock-outs, war, natural calamities or any other cause beyond its control and without its fault or negligence. The Party claiming the relief under force majeure shall notify the other Party thereof without undue delay and if the impediment continues for more than three (3) months due to such causes as mentioned above, either party shall be entitled to terminate the Contract by written notice to the other party without incurring any liability for breach of contract.

**xiii) Rejection of Bids:** In addition to rejection of bids for any reasons mentioned in the tender document, the bid is liable for rejection for the following reasons.

- Bid not submitted in accordance with this document.
- Bid is received in incomplete form.
- Bid is not accompanied by all requisite documents.
- Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period, if any.
- In case any party submits multiple proposals.

# ANNEXURE I

## Bidder Information

(Please submit this in your letter head along with technical bid)

Bidder's Name:

[Address and Contact Details]

Tender Document No. Tender No./\_\_\_\_\_;

Date:

Tender Title:

*Note: Bidder's wrong or misleading information may result in bid being rejected as nonresponsive, in addition to other punitive actions provided for such misdemeanours in the Tender Document.*

Bidder/ Contractor particulars:

(a) Name of the Company:

(b) Legal Entity of Bidder (Proprietorship  
/Partnerships /Private Company

/Government Institutions:

(c) Place of Registration/ Principal place of business/ manufacture:

(d) Complete Postal Address:

(e) Pin code/ ZIP code:

(f) Telephone nos. (with area codes):

(g) Mobile Nos.:

(h) Contact persons/ Designation:

(i) Email IDs:

Taxation Registrations:

(j) PAN number:

(k) GSTIN number:

Bidder's Authorized Representative Information

Name:

Address:

Telephone/ Mobile numbers:

Email Address:

(Signature)

(Name, designation, and seal of company)

## ANNEXURE II

Undertaking

(Please submit this in your letter head along with technical bid)

To,  
**Campus Computer Manager**  
**Indian Institute of Management Bangalore**  
**Bannerghatta Road**  
Bangalore-560076

Tender Ref No:

(Tender For \_\_\_\_\_)

Sir,

- i. I /We hereby submit our bid for.....along with other required documents.
- ii. This is to certify that I/We before submitting this bid have read and fully understood all the terms and conditions, Scope of Service and instructions contained therein and undertake myself / ourselves abide by all of them.
- iii. Our bid is valid for 120 days from the date of opening of Technical Bid.

Yours faithfully,

(Signature)

(Name, designation, and seal of company)

Date:

## ANNEXURE III

DECLARATION REGARDING BLACKLISTING / DEBARRING FOR TAKING PART IN TENDER  
(Please submit this in your letter head along with technical bid)

To

**Campus Computer Manager**  
**Indian Institute of Management Bangalore**  
**Bannerghatta Road**  
Bangalore-560076

I / We..... **(name of the bidder)** hereby declare that the bidder / bidder namely M/s ..... **(name of the firm/company of the bidder)** has not been blacklisted or debarred in the past by Union / State Government or organization from taking part in Government tenders in India and should not have any litigation in any of the labour courts.

**OR**

I / We ..... **(name of the bidder)** hereby declare that the bidder / bidder namely M/s ..... **(name of the bidder of the bidder)** was blacklisted or debarred by Union / State Government or any organization from taking part in Government tenders for a period of ..... years w.e.f. .... To ..... The period has been completed on ..... and now the bidder / bidder is entitled to take part in Government tenders.

In case the above information is found false, I / We are fully aware that the tender / contract will be rejected / cancelled by the Institute and the EMD submitted by the bidder will be forfeited. In addition to the above, Institute will not be responsible to pay the bills for any completed / partially completed work.

(Signature)

(Name, designation, and seal of company)

Date:

## ANNEXURE IV

Bank Guarantee towards EMD  
(Please submit this in your letter head along with technical bid)

Whereas \_\_\_\_\_ (hereinafter called the bidder”) has submitted their offer dated \_\_\_\_\_ for the supply of \_\_\_\_\_ (hereinafter called the tender”) against the purchaser’s tender enquiry No. \_\_\_\_\_

KNOW ALL MEN by these presents that WE \_\_\_\_\_ of having our registered office at \_\_\_\_\_

are bound unto \_\_\_\_\_ (hereinafter called the “Purchaser”)

In the sum of \_\_\_\_\_

for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this \_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_.

THE CONDITIONS OF THIS OBLIGATION ARE:

(1) If the bidder withdraws or amends or modifies or impairs or derogates from the Tender in any respect within the period of validity of this tender.

Or

(2) If the bidder having been notified of the acceptance of his tender by the Purchaser during the period of its validity:-

(a) If the bidder fails to furnish the Performance Security for the due performance of the contract.

(b) Fails or refuses to accept/execute the contract.

WE undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 120 days after the opening of technical bids i.e., up to..... and any demand in respect thereof should reach the Bank not later than this date.

\_\_\_\_\_  
(Signature of the authorized officer of the Bank)

# ANNEXURE V

## VENDOR BANK DETAIL FORM

(Please submit this in your letter head along with technical bid)

The Indian Institute of management Bangalore  
Bannerghatta Road  
Bangalore – 560 076

Dear Sir,

I / We hereby request you to remit our payments to our bank account as per the details furnished below:

Sl. No.	Particulars	Details
1	Name of the Agency /Company	
2	Complete Address	
3	Name of the Contact Person	
4	Contact Numbers and Email ID	
5	Savings /current Account No.	
6	Name of the Bank	
7	Name of the branch with complete address	
8	IFSC Code	
9	PAN Number	

I / we hereby declare that I /we are authorized to sign this form and that the particulars furnished above are correct and complete in all respects. If the transaction is delayed or not effected at all for reasons of incomplete or incorrect information, I /we shall not hold IIMB responsible.

*Please find enclosed a cancelled cheque for your reference.*

Authorized Signatory:  
Banker

Name:

Designation:

Date:

Signature Attested by

Name:

Designation:

Date:

# ANNEXURE VI

## **DECLARATION LETTER**

(Please submit this in your letter head along with technical bid)

To

Indian Institute of Management Bangalore  
Bannerghatta Road  
Bangalore - 560 076

**SUB: ENGAGEMENT for ISO Readiness, DPDP Compliance & Security Enhancement  
(IIMB Shield 2026)**

Dear Sir,

Please find herewith enclosed the Technical Bid document comprising of Terms & conditions, General & Special Conditions and Safety Code relating to the works specified in the Technical Bid Document hereinafter set out and having acquired the requisite information relating thereto as affecting the Technical Bid, I / We hereby offer to execute the works specified in the said document in accordance with the conditions, scope of work & instructions in writing referred to in conditions of Technical Bid, articles of agreement, general conditions of contract, annexures, safety conditions and in all other respects in accordance with such conditions so far as they may be applicable.

**The document being read and understood all the contents of the Technical Bid Document do hereby accept all the Terms and conditions laid down in the said Technical Bid document and will abide by the same on acceptance and award of work.**

*Yours faithfully,*

**FOR M/s** \_\_\_\_\_

***Sign and Seal of the Company/Firm***

## ANNEXURE VII

Previous Work Experience  
(Please submit this in your letter head along with technical bid)

The bidder should have successfully executed at least five similar assignments (ISO 27001:2022 readiness & cybersecurity implementation (more than 1000 users) based on the RFP, which must have been conducted by 31 March 2025.

Sl.No	Name of the Institute	Number of Candidates that participated in the Exam	Reference Document name and Page number.
Five similar assignments for more than 1000 users			
1			
2			
3			
4			
5			

**FOR M/s** \_\_\_\_\_

**Sign and Seal of the Company/Firm**

## ANNEXURE VIII

### Financial Turnover

(Please submit this in your letter head along with technical bid)

The minimum average annual financial turnover during the last three financial years ending 31st March 2025 should be 50 lacs

FY	2022-23	2023-24	2024-25
Annual Turnover			

(Signature)

(Name, designation, and seal of company)