OIL INDIA LIMITED
(A Government of India Enterprise)
P.O. Duliajan, Pin – 786602
Dist-Dibrugarh, Assam

CORRIGENDUM NO. 4 DATED 14.10.2023

To

BID NO. GEM/2023/B/3804613 dated 09-08-2023 for Hiring of Consultancy services to develop Cybersecurity at OIL.

This Corrigendum is issued to notify the following changes:

1. Extension of dates:

- Last Date of Bid Submission is **31.10.2023 (14:00 Hrs IST)**
- Last Date of Bid Opening is **31.10.2023 (14:30 Hrs IST)**

2. The following documents have been newly uploaded in GeM Portal as replacements of the earlier:

- PQC/BEC/BRC REVISED
- CHECKLIST FOR QCBS
- ANNEXURE-I REVISED (EXPERIENCE STATEMENT OF BIDDER/SERVICE PROVIDER)
- ANNEXURE-II REVISED (PROFORMA FOR CURRICULUM VITAE OF KEY PERSONNEL)
- CHECKLIST FOR BEC-BRC REVISED
- SECTION-II SPECIAL CONDITIONS OF CONTRACT (SCC) REVISED
- SECTION-III SCOPE OF WORK (SOW) REVISED

All other terms and conditions of the Bid Document remain unchanged. Details can be viewed at www.oil-india.com.

PRE-QUALIFICATION CRITERIA/BID EVALUATION CRITERIA (BEC)/BID REJECTION CRITERIA (BRC) REVISED

1.0 BID EVALUATION CRITERIA (BEC):

The bid shall conform generally to the specifications and terms and conditions given in this bid document. Bids shall be rejected in case the services offered do not conform to required parameters stipulated in the technical specifications. Notwithstanding the general conformity of the bids to the stipulated specifications, the following requirements shall have to be particularly met by the bidders without which the same shall be considered as non-responsive and rejected. All the documents related to BEC must be submitted along with the techno-commercial Bid.

2.0 ELIGIBILITY CRITERIA:

The bidder must be incorporated/registered in India and must maintain more than or equal to 20% local content (LC) for the offered services to be eligible to bid against this tender.

Regarding calculation of local content and submission of documents during bidding & execution of contracts, provision of Public Procurement (Preference to Make in India) Order, 2017 of Department for Promotion of Industry and Internal Trade (DPIIT), Govt. of India as revised vide Order No. P45021/2/2017-PP (BE-II) dated 16th September 2020 (and as amended time to time) with modifications as notified vide MoP&NG Order No. FP-20013/2/2017-FP-PNG-Part (4) (E-41432) dated 26th April 2022, shall be applicable.

Whether or not the bidders want to avail PP-LC benefit against this tender, it is mandatory for them to meet the following at the bidding stage:

(a) The bidder must provide the percentage (%) of local content in their bid, without which the bid shall be liable for rejection being non-compliant.

(b) The Bidder shall submit an undertaking from the authorised signatory of bidder having the Power of Attorney along with the bid specifying the LC Percentage and such undertaking shall become a part of the contract, if awarded. [Format enclosed as **PROFORMA-XIII**].

(c) Bidder to submit a copy of their Certificate of Incorporation/registration in India.

3.0 TECHNICAL CRITERIA:

The bidder must be a consultancy firm having experience in providing the services below either in single or maximum two nos. of contracts of minimum value of **Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand)** only, during the last 07 (Seven) years reckoned from the original bid closing date in Central Govt./State Govt./Public Sector Undertaking/State Govt. Enterprise/ Public Limited Company, in India:

i) **Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for ICT or IT (Information and Communications Technology or Information Technology) systems.**

AND

ii) **Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for OT (Operational Technology) systems.**

Notes to BEC Clause 3.0 above:

A) In support of the experience mentioned above (Clause No. 3.0), the service provider/bidder must furnish the details of the Contracts executed by them in tabular form in **ANNEXURE-I** along with self-attested photocopies of the following documentary evidence(s):

(i) Contract(s) [Relevant pages of the Contract(s) executed]/Work-order(s)/service order(s)/Letter of Award(s)/Letter of Intent(s) indicating Scope of service(s), work, contract period.

AND

(ii) Completion certificate(s)/Final Payment certificate(s) issued by the client(s) for each of the above Contracts or any other document(s), which can substantiate the successful execution of work.

B) The bidder shall provide valid certificates from CERT-IN in their offer confirming that the bidder is currently empaneled by CERT-In as Information Security Auditing Organization, along with an undertaking to maintain its validity throughout the contract period.

C) The bidder shall provide valid certificates from IS/ISO/IEC conforming that the bidder is IS/ISO/IEC 27001:2013 or IS/ISO/IEC 27001:2022 certified, along with an undertaking to maintain its validity throughout the contract period.

D) Following work experience shall also be taken into consideration:

i) If the prospective bidder is executing work (as mentioned in Clause No. 3.0), which is still running, and the contract value executed prior to original bid closing date can be shown under experience value for the qualification under the BEC.

ii) In case the start date of the requisite experience is beyond the prescribed 07 (Seven) years reckoned from the original bid closing date, but completion is within the prescribed 07 (Seven) years reckoned from the original bid closing date. However, the value of work done during the prescribed 07 (Seven) years

period from the original bid closing date can be shown under experience value for the qualification under the BEC.

iii) If the prospective bidder has executed contract in which work (as mentioned under Clause No. 3.0) is a component of the contract.

- In case the document submitted as per **Para (A)** above are not sufficient to establish the value/period of the work experience mentioned in **Para D, i), ii) & iii)** above, the bidder shall also have to submit the breakup of the works executed under such contract(s) clearly indicating the value/period of work (as mentioned in Clause No. 3.0) which should be certified by the end user or a certificate issued by a practicing Chartered/Cost Accountant Firm (with Membership Number & Firm Registration Number).

E) Experience of executing work (as mentioned under Clause No. 3.0) through 'sub-contracting' shall not be considered for evaluation.

F) A job executed by a bidder or its partnering company for their own organization or respective subsidiary shall not be considered as experience for meeting the BEC.

G) Bidding through Joint Venture (JV) & Consortium is not acceptable.

4.0 CORE TEAM EXPERIENCE

As a part of the project execution, bidder shall deploy the followings:

A) A **Consultant's Steering Committee Member**. In this regard, the bidder shall submit the Curriculum Vitae (CV) of the proposed personnel as per **Annexure-II** along with their offer. The CV must contain the following information:

- Employee ID.
- Date of Birth
- Educational qualification
- Experience
- Industry Certificate with Number/ID

To ascertain the competency of offered personnel, CV shall be evaluated based on qualification and experience criteria as below:

i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1 (Clause No. 3.1.2 I) of SOW)

ii) Experience: The Consultant's Steering Committee Member must have an experience of minimum 15 years to be reckoned from the original bid closing date in various cyber security roles with at least 05 (Five) years of experience in cybersecurity risk assessment projects.

B) A **Delivery Team** comprising of 01 No. Project Manager, 02 Nos. Subject Matter Expert – ICT Security, 02 Nos. Subject Matter Expert – OT/ICS Security, 01 No. Subject Matter Expert – Cybersecurity Governance and shall submit the Curriculum

Vitae (CV) of the proposed personnels as per **Annexure-II** along with their offer. The CV must contain the following information:

- Employee ID
- Date of Birth
- Educational Qualification
- Experience
- Industry Certificate with Number/ID

To ascertain the competency of offered personnels, CVs shall be evaluated based on qualification and experience criteria as below:

a) **01 No. Project Manager**

i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1 (Clause No. 3.1.2 I) of SOW)

ii) Experience: The Project Manager must have an experience of minimum 10 (Ten) years to be reckoned from the original bid closing date in various cybersecurity roles with at least 03 (Three) years of experience in cybersecurity risk assessment projects.

b) **02 Nos. Subject Matter Expert – ICT Security**

i) Qualification: BE/BTech with at least any three distinct certificates from Pool-2 (Clause No. 3.1.2 I) of SOW) must be available among the members of the team (including any additional manpower deployed by the bidder).

ii) Experience: The **Subject Matter Experts – ICT Security** must have an experience of minimum 07 years to be reckoned from the original bid closing date in various roles in IT security with at least 02 years of experience in cybersecurity risk assessment projects.

c) **02 Nos. Subject Matter Expert – OT/ICS Security**

i) Qualification: BE/BTech with at least any two of the certificates from Pool-3 (Clause No. 3.1.2 I) of SOW) must be available among the members of the team (including any additional manpower deployed by the bidder).

ii) Experience: The **Subject Matter Experts – OT/ICS Security** must have an experience of minimum 05 years to be reckoned from the original bid closing date in various roles in in various roles in various roles in OT/ICS security with at least 02 years of experience in cybersecurity risk assessment projects.

d) **01 No. Subject Matter Expert – Cybersecurity Governance**

i) Qualification: MBA/BE/BTech/Law graduate with at least any one of the certificates from Pool-1/Pool-4 (Clause No. 3.1.2 I) of SOW)

ii) Experience: The **Subject Matter Experts – OT/ICS Security** must have an experience of minimum 05 years to be reckoned from the original bid closing date in various roles in the field of cybersecurity governance, risk, and compliance.

C) A **Quality Assurance Team** comprising of 01 No. QA Lead and 02 Nos. Quality Reviewers and shall submit the Curriculum Vitae (CV) of the proposed personnels as per **Annexure-II** along with their offer. The CV must contain the following information:

- Employee ID
- Date of Birth
- Educational Qualification
- Experience
- Industry Certificate with Number/ID

To ascertain the competency of offered personnels, CVs shall be evaluated based on qualification and experience criteria as below:

a) **01 No. QA Lead**

i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1/Pool-2/Pool-3 (Clause No. 3.1.2 I) of SOW)

ii) Experience: The **QA Lead** must have an experience of minimum 10 years to be reckoned from the original bid closing date in various cybersecurity roles.

b) **02 Nos. Quality Reviewers**

i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1/Pool-2/Pool-3/Pool-4 (Clause No. 3.1.2 I) of SOW)

ii) Experience: The **Quality Reviewers** must have an experience of minimum 5 years to be reckoned from the original bid closing date in various roles in OT/ICS security.

Note:

The CVs should be certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney. Service Provider/Bidder should submit CVs for at least the specified nos. of qualified **personnels** as above (Clause 4.0 A, B and C). Failing to provide the same, the bid shall be considered as non-responsive and shall be liable for rejection. However, bidder can propose/offer more than requisite number of personnels as indicated above for selection/consideration by the company under this tender.

5.0 QUALITY & COST BASED SELECTION (QCBS)-SCORING AND EVALUATION CRITERIA

Bids which are techno-commercially and financially qualified shall be evaluated both in terms of quality as well as quoted price i.e., Quality & Cost Based Selection (QCBS) methodology. The weightage for quality is 70 and the weightage for the quoted price is 30 i.e., Quality: Quoted price is 70:30. Competency of the bidder shall be evaluated through the QCBS matrix as indicated below:

Sl No.	Quality Criteria		Marks
1.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for ICT or IT (Information and Communications Technology or Information Technology) systems'** of minimum value **Rs. 50,00,000.00 (Rupees Fifty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.		**20 (max)**
1. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20	
1. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16	
1. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12	
2.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for OT (Operational Technology) systems'** of minimum value **Rs. 30,00,000.00 (Rupees Thirty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.		**20 (max)**
2. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20	
2. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16	
2. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12	

Note to SL Nos. 1. And 2. of QCBS:

1. The bidder should submit copies of Contracts/PO's along with completion certificates and/or payment receipts along with the technical bid to substantiate the above.

2. If the bidder has experience in providing 'cybersecurity consultancy services for both ICT (Information and Communications Technology) systems and OT (Operational Technology) systems in a single project, the same project shall be considered for marking against both Sl. Nos. 1 and 2 above.

3.	**Team composition of Project Delivery Team**		**60 (max)**
3.1	**Experience of Project Manager**		**16 (max)**
3.1 a)	Experience of 15 (Fifteen) years or more to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	16	
3.1 b)	Experience of more than 10 (Ten) years but less than 15 (Fifteen) years or more from to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15.5	
3.1 c)	Experience of 10 (Ten) years to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15	
3.2	**Deployment of Subject Matter Experts**		**12 (max)**
3.2.1	**Subject Matter Expert – ICT Security**		04 (max)
3.2.1 a)	05 (Five) or more nos. of Subject Matter Experts in ICT Security.	4	
3.2.1 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in ICT Security.	3.5	
3.2.1 c)	02 (Two) nos. of Subject Matter Experts in ICT Security.	3	
3.2.2	**Subject Matter Expert – OT/ICS Security**		04 (max)
3.2.2 a)	05 (Five) or more nos. of Subject Matter Experts in OI/ICS Security.	4	
3.2.2 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in OI/ICS Security.	3.5	
3.2.2 c)	02 (Two) nos. of Subject Matter Experts each in OI/ICS Security.	3	
3.2.3	**Subject Matter Expert – Cybersecurity Governance**		04 (max)
3.2.3 a)	03 (Three) or more nos. of Subject Matter Expert – Cybersecurity Governance	4	
3.2.3 b)	02 (Two) nos. of Subject Matter Experts – Cybersecurity Governance	3.5	
3.2.3 c)	01 (One) no. Subject Matter Expert – Cybersecurity Governance	3	

3.2.4	**Total cumulative experience of the subject matter experts (i.e., experience of 02 nos. ICT Security experts + 02 nos. OT/ICS Security experts + 01 no. of Cybersecurity Governance expert) of the Project Delivery Team in various cybersecurity roles as per their respective qualification criteria in Clause No. 4.0 B).**		**16 (max)**
3.2.4 a)	Experience of 35 years or more to be reckoned from the original bid closing date.	16	
3.2.4 b)	Experience of more than 29 years but less than 35 years to be reckoned from the original bid closing date.	15.5	
3.2.4 c)	Experience of 29 years to be reckoned from the original bid closing date.	15	
3.2.5	**Industry Certificate** **Team members (excluding the Project Manager) with acceptable industry certificates.**		**16 (max)**
3.2.5.1	**Certificate from Pool-1**		4 (max)
a)	03 or more distinct certificates from Pool-1	4	
b)	02 distinct certificates from Pool-1	3.5	
c)	01 distinct certificate from Pool-1	3	
3.2.5.2	**Certificate from Pool-2**		
a)	06 or more distinct certificates from Pool-2	4	4 (max)
b)	04 to 05 distinct certificates from Pool-2	3.5	
c)	03 distinct certificates from Pool-2	3	
3.2.5.3	**Certificate from Pool-3**		
a)	04 or more distinct certificates from Pool-3	4	4 (max)
b)	03 distinct certificates from Pool-3	3.5	
c)	02 distinct certificate from Pool-3	3	
3.2.5.4	**Certificate from Pool-4**		4 (max)
a)	03 or more distinct certificates from Pool-3	4	
b)	02 distinct certificates from Pool-3	3.5	
c)	01 distinct certificate from Pool-3	3	

Note to SL No. 3:

1. Any additional human resources to be deployed must meet the corresponding minimum qualification criteria as mentioned under Clause No. 4.0 above.

2. To substantiate this, the bidder must submit CVs including copies of the industry certificates and qualifications of the proposed team members, certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney, along with the bid.

	TOTAL		**100 (MAX)**

Notes:

i) It shall be the bidder's responsibility to ensure submission of unambiguous/clear and sufficient documentary evidence in support of the evaluation criteria/QCBS.

ii) OIL reserves the right to verify any or all data/document/information provided by the bidder. False statement by bidder shall make it liable for appropriate action.

iii) It may be noted that OIL shall not seek any clarification against the documents submitted by the bidder to substantiate the QCBS score (quality parameters tabulated above), after the technical bid opening. Therefore, bidders must ensure that such documents (in toto) are submitted as part of the original submission. **Also, the bidders must indicate – (i) Details of the document (Document Ref. No., relevant Pg. No. etc.) submitted & (ii) Marks Claimed by the bidder against each Quality parameter, in the format prescribed in 'QCBS CHECKLIST' and submit the same along with the technical bid**.

iv) A bid shall have to meet the **Minimum Qualifying Marks of 75 in 'Quality' Criteria**. The Bids meeting the minimum qualifying marks shall be called 'Qualified Bids' and shall be eligible for price evaluation of the bid.

v) Since bidder's qualification marks are linked with the qualification & experience of Core Team, bidders should ensure that the same persons, whose CV's are part of the offer are deployed during the execution of the Project. An undertaking in this respect to be provided by the bidder. Bidders are free to quote for multiple persons against the personnels of the Core Team meeting the experience & qualification criteria. However, for marking against QCBS, person with least qualifications (relevant experience in terms of years) shall be considered.

6.0 FINANCIAL CRITERIA:

6.1 Annual Financial Turnover of the bidder during any of preceding 03 (Three) financial/accounting years from the original bid closing date should be at least **Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand)** only.

6.2 Net worth of the bidder must be Positive for the preceding financial/accounting year.

Note:

i. Annual Financial Turnover of the bidder from operations shall mean: 'Aggregate value of the realisation of amount made from the sale, supply or distribution of goods or on account of services rendered, or both, by the company (bidder) during a financial year' as per the Companies Act, 2013 Section 2 (91).

ii. Net worth shall mean: 'Share capital + Reserves created out of profits and securities Premium - Aggregate value of accumulated losses (excluding revaluation reserves) - deferred expenditure - Miscellaneous Expenditure to

the extent not written off and carried forward Loss - Reserves created out of write back of depreciation and amalgamation'.

Notes to BEC Clause No. 6.0:

a. For proof of Annual Turnover & Net worth, any one of the following documents/photocopies must be submitted along with the bid:

(i) Audited Balance Sheet along with Profit & Loss account.

OR

(ii) A certificate issued by a practicing Chartered/Cost Accountant (with Membership Number and Firm Registration Number), as per format prescribed in **PROFORMA-IX**.

Note: Mention of UDIN (Unique Document Identification Number) is mandatory for all Certificates issued w.e.f. February 1, 2019 by Chartered Accountant in Practice.

b. Considering the time required for preparation of Financial Statements, if the last date of preceding financial/accounting year falls within the preceding six months/within the due date for furnishing of audit report as per Section 139(1) of IT Act, 1961 (read along with latest circulars/notifications issued by CBDT from time to time) reckoned from the original bid closing date and the Financial Statements of the preceding financial/accounting year are not available with the bidder, then the financial turnover of the previous three financial/accounting years excluding the preceding financial/accounting year will be considered. In such cases, the Net worth of the previous financial/accounting year excluding the preceding financial/accounting year will be considered. However, the bidder has to submit an undertaking in support of the same along with their technical bid as per **PROFORMA-X**.

c. In case the bidder is a Central Govt. Organization/PSU/State Govt. Organization/Semi-State Govt. Organization or any other Central/State Govt. Undertaking, where the auditor is appointed only after the approval of Comptroller and Auditor General of India and the Central Government, their certificates may be accepted even though FRN is not available. However, bidder to provide documentary evidence for the same.

d. In case the bidder is a Government Department, they are exempted from submission of document mentioned under para **a.** and **b.** above.

e. Bid shall be rejected if not accompanied with adequate documentary proof in support of Annual turnover and Net worth as mentioned in Para 6.1 & 6.2.

7.0 COMMERCIAL EVALUATION CRITERIA:

7.1 The bids are to be submitted in single stage under Two Bid System i.e., Un-priced Techno-Commercial Bid and Price Bid together. The Un-priced techno-commercial bid (or Technical bid) must comprise of all the technical documents substantiating the previous experience, financial & technical credentials of the bidder and any other

document as asked for in the bid document. **There should not be any indication of price in the Technical bid; otherwise, the bid shall be rejected straightaway.**

7.2 **Bidders must fill the 'PRICE BIDDING FORMAT/FINANCIAL DOCUMENT' and compute all-inclusive (including GST) bid value. This all-inclusive (including GST) bid value is to be entered against the 'OFFER PRICE' field in the GeM portal. The duly filled 'PRICE BID/FINANCIAL DOCUMENT' in electronic form must be submitted by the bidders through GeM Portal only along with the Financial Bid. Any Financial Bid without the duly filled Price Bid shall be liable for rejection.]**
Note: The breakup of the quoted/offered price i.e. the duly filled Price Bid Format MUST NOT be uploaded with the technical bid; otherwise the bid shall be rejected straightway.

7.3 The quantities shown against each item in the BOQ shall be considered for the purpose of Bid Evaluation. It is, however, to be clearly understood that the assumptions made in respect of the quantities for various operations are only for the purpose of evaluation of the bid and the Contractor will be paid on the basis of the actual Quantity consumed, as the case may be.

7.4 The price quoted by the successful bidder must be firm during the performance of the contract and not subject to variation on any account except as mentioned in the bid document. Any bid submitted with adjustable price quotation other than the above will be treated as non-responsive and rejected.

7.5 Bid security shall be furnished as a part of the Techno Commercial Un-Priced Bid. The amount of bid security should be as specified in the Forwarding letter/Introduction/GeM bid document. Any bid not accompanied by a proper bid security will be rejected.

7.6 Any bid received in the form of Physical document/Telex/Cable/Fax/E-mail will not be accepted.

7.7 Bids shall be typed or written in indelible ink.

7.8 Bids shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by bidder, in which case such corrections shall be initiated by the authorized signatory. However, white fluid should not be used for making corrections. Any bid not meeting this requirement shall be rejected.

7.9 Any bid containing false statement will be rejected and action will be taken by Company as per Bid Document.

7.10 Bidder must accept and comply with the following provisions as given in the Tender Document in toto, failing which offer will be rejected:

(i) Firm price
(ii) Bid Securing Declaration
(iii) Period of validity of Bid

(iv) Price Schedule
(v) Performance Bank Guarantee/Security deposit
(vi) Delivery/Completion Schedule
(vii) Scope of work
(viii) Guarantee of material/work
(ix) Liquidated Damages clause
(x) Tax liabilities
(xi) Arbitration/Resolution of Dispute Clause
(xii) Force Majeure
(xiii) Applicable Laws
(xiv) Specifications
(xv) Integrity Pact

7.11 There should not be any indication of price in the Un-priced Techno-Commercial Bid. A bid will be straightway rejected if this is given in the Un-priced Techno-Commercial Bid.

7.12 Bid received with validity of offer less than 120 (One Hundred and Twenty) days from Bid Opening Date will be rejected.

7.13 The Integrity Pact is applicable against this tender. OIL shall be entering into an Integrity Pact with the bidders as per format enclosed vide "**Integrity Pact**" of the tender document. The proforma has to be returned by the bidder (along with the Un-priced Techno-Commercial Bid) duly signed by the same signatory who signed the bid, i.e., who is duly authorized to sign the bid. Uploading the Integrity Pact with digital signature will be construed that all pages of the Integrity Pact have been signed by the bidder's authorized signatory who sign the Bid.

8.0 QSBS EVALUATION CRITERIA:

8.1 The bids conforming to the technical specifications, terms and conditions stipulated in the bidding document and considered to be responsive after subjecting to Evaluation Criteria mentioned above shall be considered for QCBS evaluation as per criteria given below:

8.2 Bids shall be evaluated both in terms of Quality (as per Para 5.0 above) as well as Quoted Price i.e., Quality & Cost Based Selection (QCBS) methodology. **The weightage for Quality is 70 and the weightage for the Quoted price is 30.**

9.0 PRICE BID EVALUATION:

9.1 The Qualified Bids **(meeting the minimum Qualifying Marks of 75 in Quality Criteria)** and conforming to the technical specifications, terms and conditions stipulated in the bidding document and considered to be responsive after subjecting to Bid Evaluation Criteria mentioned above shall be considered for price evaluation.

9.2 Quoted unit rates against each Line Item of the price bidding format shall be considered only up to 2 decimal places without rounding off for evaluation. In case

the unit rate against a line item is found blank, the cost of that particular service shall be considered as inclusive in the total offered price.

9.3 The bidders are advised not to offer any discount/rebate separately and to offer their prices in the Price Bid Format after considering discount/rebate, if any.

9.4 OIL shall prefer to deal with registered bidder under GST. Therefore, bidders are requested to get themselves registered under GST, if not registered yet.

However, in case any unregistered bidder is submitting their bid, their prices will be loaded with applicable GST while evaluation of bid.

9.5 When a bidder mentions taxes as extra without specifying the rates & amount, the offer will be loaded with maximum value towards taxes received against the tender for comparison purposes. If the bidder emerges as lowest bidder after such loading, in the event of order on that bidder, taxes mentioned by OIL on the Purchase Order/Contracts will be binding on the bidder.

9.6 Input Tax Credit on GST (Goods & Service Tax) for this service is NOT available to OIL & the bids will be evaluated based on total price including GST.

9.7 Price Bid uploaded without giving any details of the taxes (Including rates and amounts) shall be considered as inclusive of all taxes including GST.

9.8 In case the GST rating of Contractor on the GST portal/Govt. official website is negative/black listed, then the bids may be rejected by OIL. Further, in case rating of bidder is negative/black listed after award of work for supply of goods/services, then OIL shall not be obligated or liable to pay or reimburse GST to such Contractor and shall also be entitled to deduct/recover such GST along with all penalties/interest, if any, incurred by OIL.

9.9 **INTER SE-RANKING OF THE QUALIFIED BIDS:**

To ascertain the inter se-ranking of the bids the Quality & Cost Based Selection (**QCBS) methodology** as mentioned below shall be adopted:

9.9.1 An **Evaluated Bid Score (B)** will be calculated for each bid, which meets the **minimum Qualifying marks of 75 in Quality Evaluation Criteria**, using the following formula in order to have a comprehensive assessment of the Bid price and the Quality of each bid:

$$\mathbf{B = (C_{low}/C)*100*X + (T/T_{high})*100*Y}$$

Where,

C = Offer Price of the bidder
C_{low} = The lowest of the Offer Price among responsive bids
T = The total marks obtained by the bidder against *Quality* criteria
T_{high} = The total marks achieved by the best bid among all responsive bids against *Quality* criteria
X = 0.30 (The weightage for *Quoted price* is 30)

Y = 0.70 (The weightage for *Quality* is 70)

Note: The **Evaluated Bid Score (B)** shall be considered up to two decimal places.

9.9.2 The bid with the **highest Evaluated Bid Score (B)** shall be **recommended for award of contract.**

9.9.3 In the event of two or more bids having the same highest Evaluated Bid Score (B), the bid scoring the highest marks against *Quality* criteria shall be given preference and shall be ranked higher. Even then, if there is tie, the selection shall be made in accordance with GeM GTC.

10.0 GENERAL:

10.1 In case bidder takes exception to any clause of bidding document not covered under BEC/BRC, then the Company has the discretion to load or reject the offer on account of such exception if the bidder does not withdraw/modify the deviation when/as advised by company. The loading so done by the company will be final and binding on the bidders. No deviation will however be accepted in the clauses covered under BEC/BRC.

10.2 To ascertain the substantial responsiveness of the bid the Company reserves the right to ask the bidder for clarification in respect of clauses covered under BEC/BRC also and such clarifications fulfilling the BEC/BRC clauses in toto must be received on or before the deadline given by the company, failing which the offer shall be evaluated based on the submission. However, mere submission of such clarification shall not make the offer responsive, unless company is satisfied with the substantial responsiveness of the offer.

10.3 If any of the clauses in the BEC/BRC contradict with other clauses of bidding document elsewhere, the clauses in the BEC/BRC shall prevail.

10.4 Bidder(s) must note that requisite information(s)/financial values etc. as required in the BEC/BRC & Tender are clearly understandable from the supporting documents submitted by the Bidder(s); otherwise, Bids shall be rejected.

10.5 OIL shall not be responsible for delay, loss or non-receipt of applications for participating in the bid sent by mail and will not entertain any correspondence in this regard.

10.6 The originals of such documents [furnished by bidder(s)] shall have to be produced by bidder(s) to OIL as and when asked for.

11.0 PURCHASE PREFERENCE CLAUSE: Purchase Preference Clause for MSE bidders as well Purchase Preference Policy – Linked with Local Content (PP-LC) shall not be applicable against this tender.

12.0 **COMPLIANCE OF THE COMPETITION ACT, 2002:** The bidder shall strictly comply with the provisions of the Competition Act, 2002, more particularly, Section-3 of the Act. Any violation the provisions of the Act shall attract penal action under the Act.

13.0 **CHECKLIST FOR BEC-BRC:** Enclosed as BEC/BRC CHECKLIST. To be submitted along with the technical bid.

End of PQC/BEC/BRC

CHECKLIST FOR QCBS

Sl No.	Quality Criteria		Marks	Bidders to indicate the following:	
				Marks claimed by the Bidder	Details of submitted Doc. (e.g. Doc Ref. No., Pg. No. etc.)
1.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for ICT or IT (Information and Communications Technology or Information Technology) systems'** of minimum value **Rs. 50,00,000.00 (Rupees Fifty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.		**20 (max)**		
2. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20			
2. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16			
2. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12			
2.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for OT (Operational Technology) systems'** of minimum value **Rs. 30,00,000.00 (Rupees Thirty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.		**20 (max)**		
2. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20			
2. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16			

2. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12			
<u>Note to SL Nos. 1. And 2. of QCBS</u>: 2. The bidder should submit copies of Contracts/PO's along with completion certificates and/or payment receipts along with the technical bid to substantiate the above. 2. If the bidder has experience in providing 'cybersecurity consultancy services for both ICT (Information and Communications Technology) systems and OT (Operational Technology) systems in a single project, the same project shall be considered for marking against both Sl. Nos. 1 and 2 above.					
3.	**Team composition of Project Delivery Team**		**60 (max)**		
3.1	**Experience of Project Manager**		**16 (max)**		
3.1 a)	Experience of 15 (Fifteen) years or more to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	16			
3.1 b)	Experience of more than 10 (Ten) years but less than 15 (Fifteen) years or more from to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15.5			
3.1 c)	Experience of 10 (Ten) years to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15			
3.2	**Deployment of Subject Matter Experts**		**12 (max)**		
3.2.1	**Subject Matter Expert – ICT Security**		04 (max)		
3.2.1 a)	05 (Five) or more nos. of Subject Matter Experts in ICT Security.	4			
3.2.1 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in ICT Security.	3.5			
3.2.1 c)	02 (Two) nos. of Subject Matter Experts in ICT Security.	3			
3.2.2	**Subject Matter Expert – OT/ICS Security**		04 (max)		
3.2.2 a)	05 (Five) or more nos. of Subject Matter Experts in OI/ICS Security.	4			

3.2.2 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in OI/ICS Security.	3.5			
3.2.2 c)	02 (Two) nos. of Subject Matter Experts each in OI/ICS Security.	3			
3.2.3	**Subject Matter Expert – Cybersecurity Governance**		04 (max)		
3.2.3 a)	03 (Three) or more nos. of Subject Matter Expert – Cybersecurity Governance	4			
3.2.3 b)	02 (Two) nos. of Subject Matter Experts – Cybersecurity Governance	3.5			
3.2.3 c)	01 (One) no. Subject Matter Expert – Cybersecurity Governance	3			
3.2.4	**Total cumulative experience of the subject matter experts (i.e., experience of 02 nos. ICT Security experts + 02 nos. OT/ICS Security experts + 01 no. of Cybersecurity Governance expert) of the Project Delivery Team in various cybersecurity roles as per their respective qualification criteria in Clause No. 4.0 B).**		**16 (max)**		
3.2.4 a)	Experience of 35 years or more to be reckoned from the original bid closing date.	16			
3.2.4 b)	Experience of more than 29 years but less than 35 years to be reckoned from the original bid closing date.	15.5			
3.2.4 c)	Experience of 29 years to be reckoned from the original bid closing date.	15			
3.2.5	**Industry Certificate** **Team members (excluding the Project Manager) with acceptable industry certificates.**		**16 (max)**		
3.2.5.1	**Certificate from Pool-1**		4 (max)		
a)	03 or more distinct certificates from Pool-1	4			
b)	02 distinct certificates from Pool-1	3.5			
c)	01 distinct certificate from Pool-1	3			
3.2.5.2	**Certificate from Pool-2**				
a)	06 or more distinct certificates from Pool-2	4	4 (max)		
b)	04 to 05 distinct certificates from Pool-2	3.5			
c)	03 distinct certificates from Pool-2	3			
3.2.5.3	**Certificate from Pool-3**				
a)	04 or more distinct certificates from Pool-3	4	4 (max)		
b)	03 distinct certificates from Pool-3	3.5			
c)	02 distinct certificate from Pool-3	3			
3.2.5.4	**Certificate from Pool-4**		4 (max)		
a)	03 or more distinct certificates from Pool-3	4			

b)	02 distinct certificates from Pool-3	3.5			
c)	01 distinct certificate from Pool-3	3			
Note to SL No. 3: 2. Any additional human resources to be deployed must meet the corresponding minimum qualification criteria as mentioned under Clause No. 4.0 above. 2. To substantiate this, the bidder must submit CVs including copies of the industry certificates and qualifications of the proposed team members, certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney, along with the bid.					
	TOTAL		**100 (MAX)**		

Notes:

i) It shall be the bidder's responsibility to ensure submission of unambiguous/clear and sufficient documentary evidence in support of the evaluation criteria/QCBS.

ii) OIL reserves the right to verify any or all data/document/information provided by the bidder. False statement by bidder shall make it liable for appropriate action.

iii) It may be noted that OIL shall not seek any clarification against the documents submitted by the bidder to substantiate the QCBS score (quality parameters tabulated above), after the technical bid opening. Therefore, bidders must ensure that such documents (in toto) are submitted as part of the original submission. **Also, the bidders must indicate – (i) Details of the document (Document Ref. No., relevant Pg. No. etc.) submitted & (ii) Marks Claimed by the bidder against each Quality parameter, in the format prescribed in 'QCBS CHECKLIST' and submit the same along with the technical bid**.

iv) A bid shall have to meet the **Minimum Qualifying Marks of 75 in 'Quality' Criteria**. The Bids meeting the minimum qualifying marks shall be called 'Qualified Bids' and shall be eligible for price evaluation of the bid.

v) Since bidder's qualification marks are linked with the qualification & experience of Core Team, bidders should ensure that the same persons, whose CV's are part of the offer are deployed during the execution of the Project. An undertaking in this respect to be provided by the bidder. Bidders are free to quote for multiple persons against the personnels of the Core Team meeting the experience & qualification criteria. However, for marking against QCBS, person with least qualifications (relevant experience in terms of years) shall be considered.

\

ANNEXURE-I REVISED

EXPERIENCE STATEMENT OF BIDDER/SERVICE PROVIDER

TENDER NO: _____

TABLE-1

Bidders' experience providing **'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program'** for either ICT (Information and Communications Technology) systems or OT (Operational Technology) systems, through 01 (One) single contract., during the last 07 (Seven) years reckoned from the original bid closing date.

Sl. No.	Contract No.	Name & Contact details of client	Place of Operation	Details Scope of Work of the Contract Executed	Commencement date of contract	Completion date of contract	Details of supporting Documents (e.g., Document Ref. No., File Name, Pg. No. etc.)
1							
2							
3							

N.B: Please add rows as required.

ANNEXURE-II REVISED

PROFORMA FOR CURRICULUM VITAE OF KEY PERSONNEL

1.	NAME	:
2.	EMPLOYEE ID	:
3.	PRESENT ADDRESS	:
4.	PERMANENT ADDRESS	:
5.	FATHER'S NAME	:
6.	NATIONALITY	:
7.	PASSPORT NO. AND VALIDITY	:
	(IN CASE OF EXPATRIATE)	:
8.	DATE OF BIRTH	:
9.	DESIGNATED POST	:
10.	EDUCATIONAL QUALIFICATION	:

Affix Passport Size Photograph

Sl. No.	Exam Passed	Institute	Board/University/Council Others	Grade/% Marks Obtained

11. HSE TRAININGS (If any) :
12. SPECIFIC KNOWLEDGE/EXPERIENCE :
(viz. cyber security risk assessment, cyber security concepts, frameworks, standards etc.)
13. WORK EXPERIENCE IN REVERSE ORDER:

Sl. No.	Name of the Company (Employer)	Designation or Post Held	Name of Client or Company with type of Service Provided	Job Role/ Description	Key Job Responsibility	Period of Service		Experience (Relevant to Cyber Security)
						From	To	

N.B.: Add rows as required. Annexure(s) may also be attached if required.

13. INDUSTRY CERTIFICATE DETAILS:

Sl. No.	Certificate	Certificate No.	Certifying Agency	Validity		Reference to Pool No. as mentioned in SOW – 3.1.2.1
				From	To	

N.B.: Add rows as required. Annexure(s) may also be attached if required.

Signature & Name of personnel

Seal of Bidder

Sig., Name & Designation of bidder

NOTE:

1. The CVs should be certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney
3. If OIL desires, original certificate needs to be furnished at the time of 1st deployment for verification.
4. Contractor shall provide the following before deploying his personnel:

a) Security clearance from Ministry of Home Affairs, Govt. of India for expatriate employees of Contractor

5. For the entire project, bidders should ensure that the same persons, whose CV's are part of the offer are deployed during the execution. In case of replacement of any person, the replacement personnel must have same or higher qualification as mentioned in this tender. The same has to be approved by OIL.

CHECKLIST FOR BEC-BRC REVISED

Bidder's Name: _____

Sl. No.	Clause No. of BEC/BRC	Description	Compliance		Bidder to indicate Relevant Page No. of their Bid to support the remarks/ compliance
			Yes	No	
1	**1.0**	**BID EVALUATION CRITERIA (BEC):** The bid shall conform generally to the specifications and terms and conditions given in this bid document. Bids shall be rejected in case the services offered do not conform to required parameters stipulated in the technical specifications. Notwithstanding the general conformity of the bids to the stipulated specifications, the following requirements shall have to be particularly met by the bidders without which the same shall be considered as non-responsive and rejected. All the documents related to BEC must be submitted along with the techno-commercial Bid.			
2	**2.0**	**ELIGIBILITY CRITERIA:** The bidder must be incorporated/registered in India and must maintain more than or equal to 20% local content (LC) for the offered services to be eligible to bid against this tender. Regarding calculation of local content and submission of documents during bidding & execution of contracts, provision of Public			

		Procurement (Preference to Make in India) Order, 2017 of Department for Promotion of Industry and Internal Trade (DPIIT), Govt. of India as revised vide Order No. P45021/2/2017-PP (BE-II) dated 16th September 2020 (and as amended time to time) with modifications as notified vide MoP&NG Order No. FP-20013/2/2017-FP-PNG-Part (4) (E-41432) dated 26th April 2022, shall be applicable. Whether or not the bidders want to avail PP-LC benefit against this tender, it is mandatory for them to meet the following at the bidding stage: (a) The bidder must provide the percentage (%) of local content in their bid, without which the bid shall be liable for rejection being non-compliant. (b) The Bidder shall submit an undertaking from the authorised signatory of bidder having the Power of Attorney along with the bid specifying the LC Percentage and such undertaking shall become a part of the contract, if awarded. [Format enclosed as **PROFORMA-XIII**]. (c) Bidder to submit a copy of their Certificate of Incorporation/registration in India.			
3	**3.0**	**3.0 <u>TECHNICAL CRITERIA</u>:** The bidder must be a consultancy firm having experience in providing the services below either in single or maximum two nos. of contracts of minimum value of **Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand)** only, during the last 07 (Seven) years reckoned from the original bid closing date in Central Govt./State			

		Govt./Public Sector Undertaking/State Govt. Enterprise/Public Limited Company, in India: i) **Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for ICT or IT (Information and Communications Technology or Information Technology) systems.** **AND** ii) **Cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for OT (Operational Technology) systems.**			
4		**<u>Notes to BEC Clause 3.0 above</u>:** **A)** In support of the experience mentioned above (Clause No. 3.0), the service provider/bidder must furnish the details of the Contracts executed by them in tabular form in **ANNEXURE-I** along with self-attested photocopies of the following documentary evidence(s): (i) Contract(s) [Relevant pages of the Contract(s) executed]/Work-order(s)/service order(s)/Letter of Award(s)/Letter of Intent(s) indicating Scope of service(s), work, contract period. **AND** (ii) Completion certificate(s)/Final Payment certificate(s) issued by the client(s) for each of the above Contracts or any other document(s), which can substantiate the successful execution of work.			

		B) The bidder shall provide valid certificates from CERT-IN in their offer confirming that the bidder is currently empaneled by CERT-In as Information Security Auditing Organization, along with an undertaking to maintain its validity throughout the contract period. **C)** The bidder shall provide valid certificates from IS/ISO/IEC conforming that the bidder is IS/ISO/IEC 27001:2013 or IS/ISO/IEC 27001:2022 certified, along with an undertaking to maintain its validity throughout the contract period. **D)** Following work experience shall also be taken into consideration: i) If the prospective bidder is executing work (as mentioned in Clause No. 3.0), which is still running, and the contract value executed prior to original bid closing date can be shown under experience value for the qualification under the BEC. ii) In case the start date of the requisite experience is beyond the prescribed 07 (Seven) years reckoned from the original bid closing date, but completion is within the prescribed 07 (Seven) years reckoned from the original bid closing date. However, the value of work done during the prescribed 07 (Seven) years period from the original bid closing date can be shown under experience value for the qualification under the BEC. iii) If the prospective bidder has executed contract in which work (as mentioned under Clause No. 3.0) is a component of the contract. • In case the document submitted as per **Para (A)** above are not sufficient to establish the value/period of the work experience			

		mentioned in **Para D, i), ii) & iii)** above, the bidder shall also have to submit the breakup of the works executed under such contract(s) clearly indicating the value/period of work (as mentioned in Clause No. 3.0) which should be certified by the end user or a certificate issued by a practicing Chartered/Cost Accountant Firm (with Membership Number & Firm Registration Number). **E)** Experience of executing work (as mentioned under Clause No. 3.0) through 'sub-contracting' shall not be considered for evaluation. **F)** A job executed by a bidder or its partnering company for their own organization or respective subsidiary shall not be considered as experience for meeting the BEC. **G)** Bidding through Joint Venture (JV) & Consortium is not acceptable.			
5	**4.0**	**CORE TEAM EXPERIENCE** As a part of the project execution, bidder shall deploy the followings: **A)** A **Consultant's Steering Committee Member**. In this regard, the bidder shall submit the Curriculum Vitae (CV) of the proposed personnel as per **Annexure-II** along with their offer. The CV must contain the following information: • Employee ID. • Date of Birth • Educational qualification • Experience			

		• Industry Certificate with Number/ID To ascertain the competency of offered personnel, CV shall be evaluated based on qualification and experience criteria as below: i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1 (Clause No. 3.1.2 I) of SOW) ii) Experience: The Consultant's Steering Committee Member must have an experience of minimum 15 years to be reckoned from the original bid closing date in various cyber security roles with at least 05 (Five) years of experience in cybersecurity risk assessment projects. **B)** A **Delivery Team** comprising of 01 No. Project Manager, 02 Nos. Subject Matter Expert – ICT Security, 02 Nos. Subject Matter Expert – OT/ICS Security, 01 No. Subject Matter Expert – Cybersecurity Governance and shall submit the Curriculum Vitae (CV) of the proposed personnels as per **Annexure-II** along with their offer. The CV must contain the following information: • Employee ID • Date of Birth • Educational Qualification • Experience • Industry Certificate with Number/ID To ascertain the competency of offered personnels, CVs shall be evaluated based on qualification and experience criteria as below: a) **01 No. Project Manager**			

		i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1 (Clause No. 3.1.2 I) of SOW) ii) Experience: The Project Manager must have an experience of minimum 10 (Ten) years to be reckoned from the original bid closing date in various cybersecurity roles with at least 03 (Three) years of experience in cybersecurity risk assessment projects. b) **02 Nos. Subject Matter Expert – ICT Security** i) Qualification: BE/BTech with at least any three distinct certificates from Pool-2 (Clause No. 3.1.2 I) of SOW) must be available among the members of the team (including any additional manpower deployed by the bidder). ii) Experience: The **Subject Matter Experts – ICT Security** must have an experience of minimum 07 years to be reckoned from the original bid closing date in various roles in IT security with at least 02 years of experience in cybersecurity risk assessment projects. c) **02 Nos. Subject Matter Expert – OT/ICS Security** i) Qualification: BE/BTech with at least any two of the certificates from Pool-3 (Clause No. 3.1.2 I) of SOW) must be available among the members of the team (including any additional manpower deployed by the bidder). ii) Experience: The **Subject Matter Experts – OT/ICS Security** must have an experience of minimum 05 years to be reckoned from the original bid closing date in various roles in in various roles in various roles in OT/ICS security with at least 02 years of experience in cybersecurity risk assessment projects.			

		d) **01 No. Subject Matter Expert – Cybersecurity Governance** i) Qualification: MBA/BE/BTech/Law graduate with at least any one of the certificates from Pool-1/Pool-4 (Clause No. 3.1.2 I) of SOW) ii) Experience: The **Subject Matter Experts – OT/ICS Security** must have an experience of minimum 05 years to be reckoned from the original bid closing date in various roles in the field of cybersecurity governance, risk, and compliance. **C)** A **Quality Assurance Team** comprising of 01 No. QA Lead and 02 Nos. Quality Reviewers and shall submit the Curriculum Vitae (CV) of the proposed personnels as per **Annexure-II** along with their offer. The CV must contain the following information: • Employee ID • Date of Birth • Educational Qualification • Experience • Industry Certificate with Number/ID To ascertain the competency of offered personnels, CVs shall be evaluated based on qualification and experience criteria as below: a) **01 No. QA Lead** i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1/Pool-2/Pool-3 (Clause No. 3.1.2 I) of SOW) ii) Experience: The **QA Lead** must have an experience of minimum 10 years to be reckoned from the original bid closing date in various cybersecurity roles.			

		b) **02 Nos. Quality Reviewers** i) Qualification: MBA/BE/BTech with at least any one of the certificates from Pool-1/Pool-2/Pool-3/Pool-4 (Clause No. 3.1.2 I) of SOW) ii) Experience: The **Quality Reviewers** must have an experience of minimum 5 years to be reckoned from the original bid closing date in various roles in OT/ICS security. **Note:** The CVs should be certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney. Service Provider/Bidder should submit CVs for at least the specified nos. of qualified **personnels** as above (Clause 4.0 A, B and C). Failing to provide the same, the bid shall be considered as non-responsive and shall be liable for rejection. However, bidder can propose/offer more than requisite number of personnels as indicated above for selection/consideration by the company under this tender.			
6	**5.0**	**QUALITY & COST BASED SELECTION (QCBS)-SCORING AND EVALUATION CRITERIA** Bids which are techno-commercially and financially qualified shall be evaluated both in terms of quality as well as quoted price i.e., Quality & Cost Based Selection (QCBS) methodology. The weightage for quality is 70 and the weightage for the quoted price is 30 i.e., Quality: Quoted price is 70:30. Competency of the bidder shall be evaluated through the QCBS matrix as indicated below:			

			Sl No.	**Quality Criteria**		**Marks**		
			1.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of cybersecurity program including either gap analysis & recommendations or cyber security advisory services for ICT or IT (Information and Communications Technology or Information Technology) systems'** of minimum value **Rs. 50,00,000.00 (Rupees Fifty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.		**20 (max)**		
			1. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20			
			1. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16			
			1. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12			
			2.	**Experience in providing 'cybersecurity consultancy services for assessment of cybersecurity risk and development of**		**20 (max)**		

				cybersecurity program including either gap analysis & recommendations or cyber security advisory services for OT (Operational Technology) systems' of minimum value **Rs. 30,00,000.00 (Rupees Thirty Lakh only)** for each project/contract during the last 07 (Seven) years reckoned from the original bid closing date.					
			2. a)	Experience in providing the above experience in 05 (Five) or more nos. of contracts.	20				
			2. b)	Experience in providing the above experience in 03 (Three) to 04 (Four) contracts.	16				
			2. c)	Experience in providing the above experience in in 01 (One) to 02 (Two) contracts.	12				
			Note to SL Nos. 1. And 2. of QCBS: 1. The bidder should submit copies of Contracts/PO's along with completion certificates and/or payment receipts along with the technical bid to substantiate the above. 2. If the bidder has experience in providing 'cybersecurity consultancy services for both ICT (Information and Communications Technology) systems and OT (Operational Technology) systems in a single project, the same project shall be considered for marking against both Sl. Nos. 1 and 2 above.						

			3.	**Team composition of Project Delivery Team**		**60 (max)**			
			3.1	**Experience of Project Manager**		**16 (max)**			
			3.1 a)	Experience of 15 (Fifteen) years or more to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	16				
			3.1 b)	Experience of more than 10 (Ten) years but less than 15 (Fifteen) years or more from to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15.5				
			3.1 c)	Experience of 10 (Ten) years to be reckoned from the original bid closing date in various cybersecurity roles with at least 05 years of experience in cybersecurity risk assessment projects.	15				
			3.2	**Deployment of Subject Matter Experts**		**12 (max)**			
			3.2.1	**Subject Matter Expert – ICT Security**		04 (max)			
			3.2.1 a)	05 (Five) or more nos. of Subject Matter Experts in ICT Security.	4				
			3.2.1 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in ICT Security.	3.5				

			3.2.1 c)	02 (Two) nos. of Subject Matter Experts in ICT Security.	3				
			3.2.2	**Subject Matter Expert – OT/ICS Security**		04 (max)			
			3.2.2 a)	05 (Five) or more nos. of Subject Matter Experts in OI/ICS Security.	4				
			3.2.2 b)	03 (Three) to 04 (Four) nos. of Subject Matter Experts in OI/ICS Security.	3.5				
			3.2.2 c)	02 (Two) nos. of Subject Matter Experts each in OI/ICS Security.	3				
			3.2.3	**Subject Matter Expert – Cybersecurity Governance**		04 (max)			
			3.2.3 a)	03 (Three) or more nos. of Subject Matter Expert – Cybersecurity Governance	4				
			3.2.3 b)	02 (Two) nos. of Subject Matter Experts – Cybersecurity Governance	3.5				
			3.2.3 c)	01 (One) no. Subject Matter Expert – Cybersecurity Governance	3				
			3.2.4	**Total cumulative experience of the subject matter experts (i.e., experience of 02 nos. ICT Security experts + 02 nos. OT/ICS Security experts + 01 no. of Cybersecurity Governance expert) of the Project Delivery Team in various cybersecurity roles as per their respective qualification criteria in Clause No. 4.0 B).**		**16 (max)**			
			3.2.4 a)	Experience of 35 years or more to be reckoned from the original bid closing	16				

				date.						
			3.2.4 b)	Experience of more than 29 years but less than 35 years to be reckoned from the original bid closing date.	15.5					
			3.2.4 c)	Experience of 29 years to be reckoned from the original bid closing date.	15					
			3.2.5	**Industry Certificate** **Team members (excluding the Project Manager) with acceptable industry certificates.**		**16 (max)**				
			3.2.5.1	**Certificate from Pool-1**		4 (max)				
			a)	03 or more distinct certificates from Pool-1	4					
			b)	02 distinct certificates from Pool-1	3.5					
			c)	01 distinct certificate from Pool-1	3					
			3.2.5.2	**Certificate from Pool-2**						
			a)	06 or more distinct certificates from Pool-2	4	4 (max)				
			b)	04 to 05 distinct certificates from Pool-2	3.5					
			c)	03 distinct certificates from Pool-2	3					
			3.2.5.3	**Certificate from Pool-3**						
			a)	04 or more distinct certificates from Pool-3	4	4 (max)				
			b)	03 distinct certificates from Pool-3	3.5					

			c)	02 distinct certificate from Pool-3	3		
			3.2.5.4	**Certificate from Pool-4**		4 (max)	
			a)	03 or more distinct certificates from Pool-3	4		
			b)	02 distinct certificates from Pool-3	3.5		
			c)	01 distinct certificate from Pool-3	3		
			Note to SL No. 3: 1. Any additional human resources to be deployed must meet the corresponding minimum qualification criteria as mentioned under Clause No. 4.0 above. 2. To substantiate this, the bidder must submit CVs including copies of the industry certificates and qualifications of the proposed team members, certified by the CEO/Country Head/Chief Operating Officer/HR Head or a partner with Power of Attorney, along with the bid.				
				TOTAL		**100 (MAX)**	
		Notes: i) It shall be the bidder's responsibility to ensure submission of unambiguous/clear and sufficient documentary evidence in support of the evaluation criteria/QCBS. ii) OIL reserves the right to verify any or all data/document/information provided by the bidder. False statement by bidder shall make it liable for appropriate action.					

		iii) It may be noted that OIL shall not seek any clarification against the documents submitted by the bidder to substantiate the QCBS score (quality parameters tabulated above), after the technical bid opening. Therefore, bidders must ensure that such documents (in toto) are submitted as part of the original submission. **Also, the bidders must indicate – (i) Details of the document (Document Ref. No., relevant Pg. No. etc.) submitted & (ii) Marks Claimed by the bidder against each Quality parameter, in the format prescribed in 'QCBS CHECKLIST' and submit the same along with the technical bid**. iv) A bid shall have to meet the **Minimum Qualifying Marks of 75 in 'Quality' Criteria**. The Bids meeting the minimum qualifying marks shall be called 'Qualified Bids' and shall be eligible for price evaluation of the bid. v) Since bidder's qualification marks are linked with the qualification & experience of Core Team, bidders should ensure that the same persons, whose CV's are part of the offer are deployed during the execution of the Project. An undertaking in this respect to be provided by the bidder. Bidders are free to quote for multiple persons against the personnels of the Core Team meeting the experience & qualification criteria. However, for marking against QCBS, person with			
7	**6.0**	**FINANCIAL CRITERIA:** 6.1 Annual Financial Turnover of the bidder during any of preceding 03 (Three) financial/accounting years from the original bid closing date should be at least **Rs. 2,64,04,000.00 (Rupees Two Crore Sixty-Four Lakh Four Thousand)** only.			

		6.2 Net worth of the bidder must be Positive for the preceding financial/accounting year. Note: i. Annual Financial Turnover of the bidder from operations shall mean: 'Aggregate value of the realisation of amount made from the sale, supply or distribution of goods or on account of services rendered, or both, by the company (bidder) during a financial year' as per the Companies Act, 2013 Section 2 (91). ii. Net worth shall mean: 'Share capital + Reserves created out of profits and securities Premium - Aggregate value of accumulated losses (excluding revaluation reserves) - deferred expenditure - Miscellaneous Expenditure to the extent not written off and carried forward Loss - Reserves created out of write back of depreciation and amalgamation'. **Notes to BEC Clause No. 6.0:** **a.** For proof of Annual Turnover & Net worth, any one of the following documents/photocopies must be submitted along with the bid: (i) Audited Balance Sheet along with Profit & Loss account. OR (ii) A certificate issued by a practicing Chartered/Cost Accountant (with Membership Number and Firm Registration Number), as per format prescribed in **PROFORMA-IX**. Note: Mention of UDIN (Unique Document Identification Number) is mandatory for all Certificates issued w.e.f. February 1, 2019 by			

		Chartered Accountant in Practice. **b.** Considering the time required for preparation of Financial Statements, if the last date of preceding financial/accounting year falls within the preceding six months/within the due date for furnishing of audit report as per Section 139(1) of IT Act, 1961 (read along with latest circulars/notifications issued by CBDT from time to time) reckoned from the original bid closing date and the Financial Statements of the preceding financial/accounting year are not available with the bidder, then the financial turnover of the previous three financial/accounting years excluding the preceding financial/accounting year will be considered. In such cases, the Net worth of the previous financial/accounting year excluding the preceding financial/accounting year will be considered. However, the bidder has to submit an undertaking in support of the same along with their technical bid as per **PROFORMA-X**. **c.** In case the bidder is a Central Govt. Organization/PSU/State Govt. Organization/Semi-State Govt. Organization or any other Central/State Govt. Undertaking, where the auditor is appointed only after the approval of Comptroller and Auditor General of India and the Central Government, their certificates may be accepted even though FRN is not available. However, bidder to provide documentary evidence for the same. **d.** In case the bidder is a Government Department, they are exempted from submission of document mentioned under para **a.** and **b.** above. **e.** Bid shall be rejected if not accompanied with adequate			

		documentary proof in support of Annual turnover and Net worth as mentioned in Para 6.1 & 6.2.			
8	**7.0**	**<u>COMMERCIAL EVALUATION CRITERIA:</u>** 7.1 The bids are to be submitted in single stage under Two Bid System i.e., Un-priced Techno-Commercial Bid and Price Bid together. The Un-priced techno-commercial bid (or Technical bid) must comprise of all the technical documents substantiating the previous experience, financial & technical credentials of the bidder and any other document as asked for in the bid document. **There should not be any indication of price in the Technical bid; otherwise, the bid shall be rejected straightaway.** 7.2 **Bidders must fill the 'PRICE BIDDING FORMAT/FINANCIAL DOCUMENT' and compute all-inclusive (including GST) bid value. This all-inclusive (including GST) bid value is to be entered against the 'OFFER PRICE' field in the GeM portal. The duly filled 'PRICE BID/FINANCIAL DOCUMENT' in electronic form must be submitted by the bidders through GeM Portal only along with the Financial Bid. Any Financial Bid without the duly filled Price Bid shall be liable for rejection.]** **Note: The breakup of the quoted/offered price i.e. the duly filled Price Bid Format MUST NOT be uploaded with the technical bid; otherwise the bid shall be rejected straightway.** 7.3 The quantities shown against each item in the BOQ shall be considered for the purpose of Bid Evaluation. It is, however, to be clearly understood that the assumptions made in respect of the quantities for various operations are only for the purpose of evaluation of the bid and			

		the Contractor will be paid on the basis of the actual Quantity consumed, as the case may be. 7.4 The price quoted by the successful bidder must be firm during the performance of the contract and not subject to variation on any account except as mentioned in the bid document. Any bid submitted with adjustable price quotation other than the above will be treated as non-responsive and rejected. 7.5 Bid security shall be furnished as a part of the Techno Commercial Un-Priced Bid. The amount of bid security should be as specified in the Forwarding letter/Introduction/GeM bid document. Any bid not accompanied by a proper bid security will be rejected. 7.6 Any bid received in the form of Physical document/Telex/Cable/Fax/E-mail will not be accepted. 7.7 Bids shall be typed or written in indelible ink. 7.8 Bids shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by bidder, in which case such corrections shall be initiated by the authorized signatory. However, white fluid should not be used for making corrections. Any bid not meeting this requirement shall be rejected. 7.9 Any bid containing false statement will be rejected and action will be taken by Company as per Bid Document. 7.10 Bidder must accept and comply with the following provisions as given in the Tender Document in toto, failing which offer will be rejected:			

		(i) Firm price (ii) Bid Securing Declaration (iii) Period of validity of Bid (iv) Price Schedule (v) Performance Bank Guarantee/Security deposit (vi) Delivery/Completion Schedule (vii) Scope of work (viii) Guarantee of material/work (ix) Liquidated Damages clause (x) Tax liabilities (xi) Arbitration/Resolution of Dispute Clause (xii) Force Majeure (xiii) Applicable Laws (xiv) Specifications (xv) Integrity Pact 7.11 There should not be any indication of price in the Un-priced Techno-Commercial Bid. A bid will be straightway rejected if this is given in the Un-priced Techno-Commercial Bid. 7.12 Bid received with validity of offer less than 120 (One Hundred and Twenty) days from Bid Opening Date will be rejected. 7.13 The Integrity Pact is applicable against this tender. OIL shall be entering into an Integrity Pact with the bidders as per format enclosed vide "**Integrity Pact**" of the tender document. The proforma has to be returned by the bidder (along with the Un-priced Techno-Commercial Bid) duly signed by the same signatory who signed the bid, i.e., who is duly authorized to sign the bid. Uploading the Integrity Pact with digital			

		signature will be construed that all pages of the Integrity Pact have been signed by the bidder's authorized signatory who sign the Bid.			
9	**8.0**	**<u>QSBS EVALUATION CRITERIA</u>**: 8.1 The bids conforming to the technical specifications, terms and conditions stipulated in the bidding document and considered to be responsive after subjecting to Evaluation Criteria mentioned above shall be considered for QCBS evaluation as per criteria given below: 8.2 Bids shall be evaluated both in terms of Quality (as per Para 5.0 above) as well as Quoted Price i.e., Quality & Cost Based Selection (QCBS) methodology. **The weightage for Quality is 70 and the weightage for the Quoted price is 30.**			
	9.0	**<u>PRICE BID EVALUATION</u>:** 9.1 The Qualified Bids **(meeting the minimum Qualifying Marks of 75 in Quality Criteria)** and conforming to the technical specifications, terms and conditions stipulated in the bidding document and considered to be responsive after subjecting to Bid Evaluation Criteria mentioned above shall be considered for price evaluation. 9.2 Quoted unit rates against each Line Item of the price bidding format shall be considered only up to 2 decimal places without rounding off for evaluation. In case the unit rate against a line item is found blank, the cost of that particular service shall be considered as inclusive in the total offered price. 9.3 The bidders are advised not to offer any discount/rebate separately and to offer their prices in the Price Bid Format after considering discount/rebate, if any.			

		9.4 OIL shall prefer to deal with registered bidder under GST. Therefore, bidders are requested to get themselves registered under GST, if not registered yet. However, in case any unregistered bidder is submitting their bid, their prices will be loaded with applicable GST while evaluation of bid. 9.5 When a bidder mentions taxes as extra without specifying the rates & amount, the offer will be loaded with maximum value towards taxes received against the tender for comparison purposes. If the bidder emerges as lowest bidder after such loading, in the event of order on that bidder, taxes mentioned by OIL on the Purchase Order/Contracts will be binding on the bidder. 9.6 Input Tax Credit on GST (Goods & Service Tax) for this service is NOT available to OIL & the bids will be evaluated based on total price including GST. 9.7 Price Bid uploaded without giving any details of the taxes (Including rates and amounts) shall be considered as inclusive of all taxes including GST. 9.8 In case the GST rating of Contractor on the GST portal/Govt. official website is negative/black listed, then the bids may be rejected by OIL. Further, in case rating of bidder is negative/black listed after award of work for supply of goods/services, then OIL shall not be obligated or liable to pay or reimburse GST to such Contractor and shall also be entitled to deduct/recover such GST along with all penalties/interest, if any, incurred by OIL.			

		9.9 **INTER SE-RANKING OF THE QUALIFIED BIDS:** To ascertain the inter se-ranking of the bids the Quality & Cost Based Selection (**QCBS) methodology** as mentioned below shall be adopted: 9.9.1 An **Evaluated Bid Score (B)** will be calculated for each bid, which meets the **minimum Qualifying marks of 75 in Quality Evaluation Criteria**, using the following formula in order to have a comprehensive assessment of the Bid price and the Quality of each bid: **$B= (C_{low}/C)*100*X + (T/T_{high})*100*Y$** Where, C = Offer Price of the bidder C_{low} = The lowest of the Offer Price among responsive bids T = The total marks obtained by the bidder against *Quality* criteria T_{high} = The total marks achieved by the best bid among all responsive bids against *Quality* criteria X = 0.30 (The weightage for *Quoted price* is 30) Y = 0.70 (The weightage for *Quality* is 70) **Note:** The **Evaluated Bid Score (B)** shall be considered up to two decimal places. 9.9.2 The bid with the **highest Evaluated Bid Score (B)** shall be **recommended for award of contract.** 9.9.3 In the event of two or more bids having the same highest Evaluated Bid Score (B), the bid scoring the highest marks against			

		Quality criteria shall be given preference and shall be ranked higher. Even then, if there is tie, the selection shall be made in accordance with GeM GTC.			
	10.0	**<u>GENERAL</u>:** 10.1 In case bidder takes exception to any clause of bidding document not covered under BEC/BRC, then the Company has the discretion to load or reject the offer on account of such exception if the bidder does not withdraw/modify the deviation when/as advised by company. The loading so done by the company will be final and binding on the bidders. No deviation will however be accepted in the clauses covered under BEC/BRC. 10.2 To ascertain the substantial responsiveness of the bid the Company reserves the right to ask the bidder for clarification in respect of clauses covered under BEC/BRC also and such clarifications fulfilling the BEC/BRC clauses in toto must be received on or before the deadline given by the company, failing which the offer shall be evaluated based on the submission. However, mere submission of such clarification shall not make the offer responsive, unless company is satisfied with the substantial responsiveness of the offer. 10.3 If any of the clauses in the BEC/BRC contradict with other clauses of bidding document elsewhere, the clauses in the BEC/BRC shall prevail. 10.4 Bidder(s) must note that requisite information(s)/financial values etc. as required in the BEC/BRC & Tender are clearly understandable from the supporting documents submitted by the Bidder(s); otherwise, Bids shall be rejected.			

		10.5 OIL shall not be responsible for delay, loss or non-receipt of applications for participating in the bid sent by mail and will not entertain any correspondence in this regard. 10.6 The originals of such documents [furnished by bidder(s)] shall have to be produced by bidder(s) to OIL as and when asked for.			
	11.0	**<u>PURCHASE PREFERENCE CLAUSE</u>: Purchase Preference Clause for MSE bidders as well Purchase Preference Policy – Linked with Local Content (PP-LC) shall not be applicable against this tender**.			
	12.0	**<u>COMPLIANCE OF THE COMPETITION ACT, 2002:</u>** The bidder shall strictly comply with the provisions of the Competition Act, 2002, more particularly, Section-3 of the Act. Any violation the provisions of the Act shall attract penal action under the Act.			

SPECIAL TERMS & CONDITIONS (STC)

SECTION-II

SPECIAL CONDITIONS OF CONTRACT (SCC) REVISED

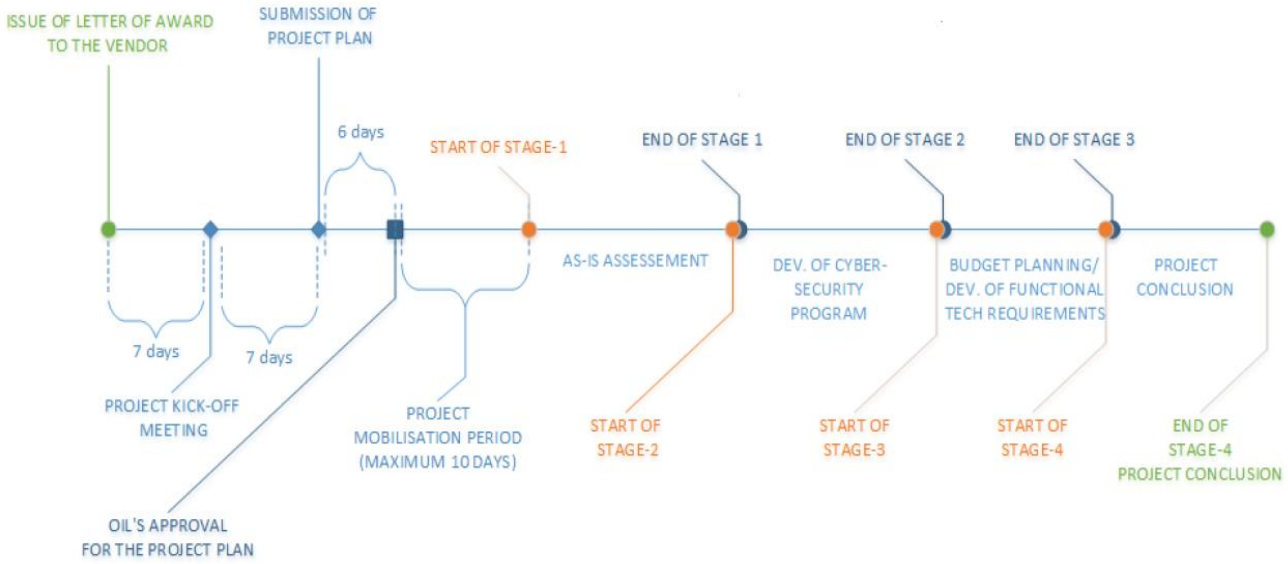
The following Special Conditions of Contract (SCC) shall supplement and/or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions herein shall prevail over those in the GCC.

Sl. no.	GCC Clause No. Ref (if any)		Clause Descriptions
1.	GCC clause no. 1.2.25	Mobilization	Mobilization should be completed within 30 (Thirty) days from the date of issuance of LOA. Contractor should complete the following activities during mobilization period as below: i) Project kick-off meeting (presentation on project execution plan) within 07 days from the date of issuance of LOA. The project kick-off meeting shall be attended by the project steering committee members along with the vendor's project delivery team and OIL core team. ii) Submission of project plan for the entire project within 14 days from the date of the date of issuance of LOA. iii) Subsequent to submission of Project Plan, OIL shall review the plan. The Contractor shall subsequently, obtain the approval from OIL for execution of their plan within 20 (Twenty) days from the date of the date of issuance of LOA. iv) Subsequent to approval of the plan, the Contractor shall mobilize their manpower for project execution within 30 (Thirty) days from the date of the date of issuance of LOA. Mobilization shall be considered as complete when the contractor is ready with all the manpower required to perform the job and upon submission of above documents.

			If the Contractor fails to mobilize within the stipulated date, the Company reserves the right to cancel the Contract without any prior notice.
2.	GCC clause no. 4.3	Duration of contract	**09 (Nine) months** from the date of Issuance of the LOA. Accordingly, the scheduled contract end date shall remain firm even in case of delayed mobilization. In case mobilization is completed before the scheduled mobilization completion date i.e., 01 (One) month, then the duration of the contract shall be considered for **08 (Eight) months** from the date of completion of actual mobilization.
3.	GCC clause no. 10	Performance Security	Upon awarding of the contract, the contractor shall furnish performance security for an amount of 10% of the Contract value within 02 (Two) weeks from the date of issuance of LOA with a validity of 03 (Three) months beyond expiry of Contract period.
4.	GCC clause no. 42.1	Arbitration	Location of Arbitration shall be Duliajan.
5.	GCC clause no. 24.0	Association of company's Personnel	OIL's representative shall advice, inspect and approve the jobs carried out by the Contractor's personnel as specified in the scope of work.
6.	GCC clause no. 30.0	Liquidated Damage Clause specific to Tender	**LIQUIDATED DAMAGES & PENALTY** In the event of the Contractor's default in timely completion of the project within the stipulated period (i.e., 09 months from date of issuance of LOA), the Contractor shall be liable to pay liquidated damages @0.5% of total contract cost per week or part thereof, of delay from date of scheduled job completion, subject to maximum of 7.5% of total contract cost. Liquidated Damages shall be reckoned from the expiry date of the scheduled job completion period.
7.	GCC clause no. 24.0	Subcontracting Allowed/Not Allowed	Not Allowed
8.		Address details for submission of invoice	All Invoices are to be sent to the following address: **GM – IT** Oil India Limited, P.O. Duliajan-786602 Dist. Dibrugarh, Assam. e-mail: sanjay@oilindia.in

9.0 Project Milestone

The following diagram describes the proposed timeline for the project.



The contract shall be executed within a period of 09 (Nine) months. The Contractor shall perform the job as per the following preferred timeline:

Milestone	(A) Allotted time period (days) to the consultant	(B) Review period for OIL (days)	Total No. of days A + B + C
Issue of Letter of Award to the vendor (D0)	—	—	0
Project Kick-off meeting (D1)	7 days from D0	—	7
Submission of Project Plan (D2)	7 days from D1	7 days	14
Mobilization Contractor's personnel (D3)	Subsequent to approval of the plan by OIL, the Contractor shall mobilize their manpower for project execution within 10 days.	—	10
Stage-1: As-Is Assessment (D4)	186 days	15 days	239 days
Stage-2: Development of the Cybersecurity Program (D5)		15 days	
Stage-3: Development of Action Plan (D6)		15 days	
Stage-4: Communication to Stakeholders and Project Closure (D7)		8 days	

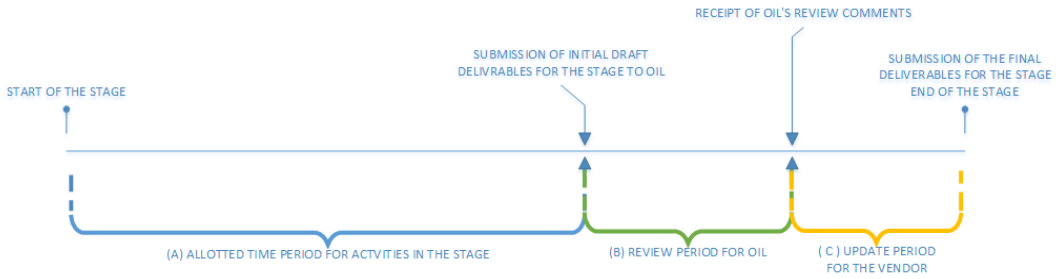
Milestone	(A) Allotted time period (days) to the consultant	(B) Review period for OIL (days)	Total No. of days A + B + C
Total Days	210 days	60	270

Notes:

i) The four stages of the project shall be executed sequentially. Each stage shall be completed in all respects (including submission of reports and other deliverables for the stage) before commencement of the next stage.

ii) The Contractor is expected to conduct the independent activities (within a stage) concurrently as much as possible, for example, different teams may perform assessments for separate functions at the same time.

iii) The following diagram describes various time periods allocated to each stage of the project.



11.0 Payment Terms

OIL shall make payment to the Contractor as per the following payment schedule.

Sl. No.	Payment Schedule	Quantum of Payment
i.	After successful completion of **Stage-1: As-Is Assessment** [Refer to the Stage conclusion checklist - 7.1.5 of Section-III SOW]	25 % of the total contract charges
ii.	After successful completion of **Stage-2: Development of the Cybersecurity Program** [Refer to the Stage conclusion checklist - 7.2.5 of Section-III SOW]	25 % of the total contract charges
iii.	After successful completion of **Stage-3: Development of Action Plan** [Refer to the Stage conclusion checklist-7.3.5 of Section-III SOW]	25 % of the total contract charges
iv.	After successful completion of **Stage-4: Communication to Stakeholders and Project Closure** [Refer to the Stage conclusion checklist - 7.4.5 of Section-III SOW]	25 % of the total contract charges

All Invoices are to be uploaded through Vendor Invoice Management portal only via the following link https://vim.oilindia.in/velocious-portal-app/
All Invoices are to be addressed to,

GM-IT, Oil India Limited, Duliajan, Assam - 786602, clearly mentioning the OIL's Work Order No. and Contract No. The amount shall be paid after deduction of penalty (if any) for the period of billing.

12.0 Responsibilities of the Contractor

1. The Contractor must complete all the activities in the project including final submission (and approval by OIL) of all deliverables within 270 (Two Hundred Seventy) days from the date of issuance of the LOA.

2. The timely completion of the work is crucial for this contract, and if the Contractor fails to meet the deadline, OIL shall be entitled to impose liquidated damages and/or penalties as outlined in Clause No. 6.o above.

3. The Contractor shall be entitled to automatic extension of time for completion of that activity, if delay, impediment or prevention caused is attributable to OIL provided the Contractor notifies OIL in writing in this regard within 07 (Seven) days of occurrence of such impediments and OIL is satisfied with the request of the Contractor.

4. Prior to starting the project, the Contractor is required to sign a confidentiality agreement that will safeguard the confidentiality of OIL's content, data, applications, structure, designs, and other information shared with or accessed by the vendor during the project execution.

5. The Contractor must ensure that all tools and software used in the project execution are licensed and legal.

6. The Contractor must make its own arrangements for transportation and accommodation of its personnel when visiting various locations of OIL within the scope of the solution. OIL shall NOT provide any transport facility or accommodation to the consultants/representatives.

7. The Contractor must provide necessary resources like laptops and Internet connectivity to its onsite project delivery team members.

8. Before deployment of human resources for any stage of the project, the Contractor shall submit their CV, copies of certificates and qualifications to OIL. OIL reserves the right to interview the proposed candidates and accept/reject their deployment. The bidder can deploy human resources only with OIL’s approval. Contractor is required to obtain permission from OIL in writing before removing any of the resources from the project.

9. Each deployed human resource must sign non-disclosure agreement (NDA) in the format provided by OIL before commencement of activities.

10. If there are any necessary personnel changes due to unforeseen circumstances, OIL's prior approval must be obtained before deployment, ensuring that the requirements for qualifications and experience specified in the tender are met. It must also be ensured that quality marks obtained against “Team Composition of Project Delivery Team” clause does not reduce due to the personnel changes.

11. The Consultant or any affiliate that directly or indirectly controls, is controlled by, or is under control with the Contractor shall be ineligible to participate in the subsequent tender(s) for providing goods, works and services resulting from or directly related to the consulting services provided in this contract.

13.0 Responsibilities of OIL

1. OIL shall provide the necessary access to its operational sites and offices to the Consultant and provide data, information as necessary under the non-disclosure agreement. Permission would be provided for taking the photographs, if any, for inclusion in the report as per the security rules of OIL. All care and effort would be made to provide the data/information as scheduled to facilitate the completion of entire work within the time limit specified in the contract.

2. Responsibility for making executive decisions related to the final acceptance of project deliverables, schedule, and other management decisions shall be entrusted to OIL's representatives in the Steering Committee.

3. The OIL's Team Lead, or Core Team members shall communicate with the Contractor's project delivery team, providing necessary information, clarifications, and resolving any issues during the contract's execution. OIL shall cooperate fully by providing details, coordinating, and obtaining approvals from various departments/divisions when necessary and appropriate.

4. OIL would ensure timely availability of internal core team to oversee the engagement.

5. It is OIL's responsibility to ensure timely approval/review feedback is given to the Consultant whenever needed, such as approving project plan, design documents, specifications, or any other necessary documents related to fulfilling the cybersecurity program.

6. OIL shall provide required authority and approval to the Consultant for performing vulnerability assessment, security testing and security configuration reviews (as required).

7. The responsibility of implementing the Consultant’s recommendations and addressing any identified gaps during the project lies with OIL.

8. OIL shall have ownership of the deliverables resulting from this engagement, except for any proprietary products or methods used by the vendor during the engagement. Both parties may utilize the concepts, techniques, and know-how developed during the course of the engagement, provided that their obligations of confidentiality are met.

9. OIL’s team and other relevant stakeholders shall be available to participate in workshops as required for the delivery of the program.

14.0 GOODS AND SERVICES TAX:

1. In view of GST Implementation from 1st July 2017, all taxes and duties including Excise Duty, CST/VAT, Service tax, Entry Tax and other indirect taxes and duties have been submerged in GST. Accordingly, reference of Excise Duty, Service Tax,

VAT, Sales Tax, Entry Tax or any other form of indirect tax except of GST mentioned in the bidding document shall be ignored.
Bidders are required to submit copy of the GST Registration Certificate while submitting the bids wherever GST (CGST & SGST/UTGST or IGST) is applicable.

2. "GST" shall mean Goods and Services Tax charged on the supply of material(s) and services. The term "GST" shall be construed to include the Integrated Goods and Services Tax (hereinafter referred to as "IGST") or Central Goods and Services Tax (hereinafter referred to as "CGST") or State Goods and Services Tax (hereinafter referred to as "SGST") or Union Territory Goods and Services Tax (hereinafter referred to as "UTGST") depending upon the import/interstate or intrastate supplies, as the case may be. It shall also mean GST compensation Cess, if applicable.

3. Quoted price/rate(s) should be inclusive of all taxes and duties, except GST (i.e. IGST or CGST and SGST/UTGST applicable in case of interstate supply or intra state supply respectively and cess on GST if applicable) on the final service. However, GST rate (including cess) to be provided in the respective places in the Price Bid. Please note that the responsibility of payment of GST (CGST & SGST or IGST or UTGST) lies with the Supplier of Goods/Services (Service Provider) only .Supplier of Goods/Services (Service Provider) providing taxable service shall issue an Invoice/Bill, as the case may be as per rules/regulation of GST. Further, returns and details required to be filled under GST laws & rules should be timely filed by Supplier of Goods/Services (Service Provider) with requisite details.

4. Bidder should also mention the Harmonised System of Nomenclature (HSN) and Service Accounting Codes (SAC) at the designated place in SOR.

5. Where the OIL is entitled to avail the input tax credit of GST:
OIL will reimburse the GST to the Supplier of Goods/Services (Service Provider) at actual against submission of Invoices as per format specified in rules/regulation of GST to enable OIL to claim input tax credit of GST paid. In case of any variation in the executed quantities, the amount on which the GST is applicable shall be modified in same proportion. Returns and details required to be filled under GST laws &rules should be timely filed by supplier with requisite details.
The input tax credit of GST quoted shall be considered for evaluation of bids, as per evaluation criteria of tender document.

6. Where the OIL is not entitled to avail/take the full input tax credit of GST:
OIL will reimburse GST to the Supplier of Goods/Services (Service Provider) at actual against submission of Invoices as per format specified in rules/regulation of GST subject to the ceiling amount of GST as quoted by the bidder. In case of any variation in the executed quantities (If directed and/or certified by the In-Charge) the ceiling amount on which GST is applicable will be modified on pro-rata basis.
The bids will be evaluated based on total price including GST.

7. Payments to Service Provider for claiming GST amount will be made provided the above formalities are fulfilled. Further, OIL may seek copies of challan and certificate from Chartered Accountant for deposit of GST collected from OIL.

8. Contractor/Contractor shall be required to issue tax invoice in accordance with GST Act and/or Rules so that input credit can be availed by OIL. In the event that the contractor/Contractor fails to provide the invoice in the form and manner prescribed under the GST Act read with GST Invoicing Rules there under, OIL shall not be liable to make any payment on account of GST against such invoice.

9. GST shall be paid against receipt of tax invoice and proof of payment of GST to government. In case of non-receipt of tax invoice or non-payment of GST by the contractor/Contractor, OIL shall withhold the payment of GST.

10. GST payable under reverse charge mechanism for specified services or goods under GST act or rules, if any, shall not be paid to the contractor/Contractor but will be directly deposited to the government by OIL.

11. Where OIL has the obligation to discharge GST liability under reverse charge mechanism and OIL has paid or is/liable to pay GST to the Government on which interest or penalties becomes payable as per GST laws for any reason which is not attributable to OIL or ITC with respect to such payments is not available to OIL for any reason which is not attributable to OIL, then OIL shall be entitled to deduct/setoff/recover such amounts against any amounts paid or payable by OIL to Contractor/Supplier.

12. Notwithstanding anything contained anywhere in the Agreement, in the event that the input tax credit of the GST charged by the Contractor/Contractor is denied by the tax authorities to OIL for reasons attributable to Contractor/Contractor, OIL shall be entitled to recover such amount from the Contractor/Contractor by way of adjustment from the next invoice. In addition to the amount of GST, OIL shall also be entitled to recover interest at the rate prescribed under GST Act and penalty, in case any penalty is imposed by the tax authorities on OIL.

13. TDS under GST, if applicable, shall be deducted from Contractor's bill at applicable rate and a certificate as per rules for tax so deducted shall be provided to the contractor/Contractor.

14. The Contractor will be under obligation for charging correct rate of tax as prescribed under the respective tax laws. Further the Contractor shall avail and pass on benefits of all exemptions/concessions available under tax laws. Any error of interpretation of applicability of taxes/duties by the contractor shall be to contractor's account.

15. It is the responsibility of the bidder to quote the correct GST rate. The classification of goods/services as per GST (Goods & Service Tax) Act should be correctly done by the contractor to ensure that input tax credit on GST (Goods & Service Tax) is not lost to the OIL on account of any error on the part of the contractor.

16. In case, the quoted information related to various taxes, duties & levies subsequently proves wrong, incorrect or misleading, OIL will have no liability to reimburse the difference in the duty/tax, if the finally assessed amount is on the higher side and OIL will have to right to recover the difference and in case the rate of duty/taxes finally assessed is on the lower side.

17. Notwithstanding anything mentioned elsewhere in the Bidding Document the aggregate liability of OIL towards Payment of Taxes & Duties shall be limited to the volume of GST declared by the bidder in its bid & nothing shall be payable extra except for the statutory variation in taxes & duties.

18. Further, it is the responsibility of the bidders to make all possible efforts to make their accounting/IT system GST compliant in order to ensure availability of Input Tax Credit (ITC) to Oil India Ltd.

19. GST liability, if any on account of supply of free samples against any tender shall be to bidder's account.

20. In case of statutory variation in GST, other than due to change in turnover, payable on the contract value during contract period, the Supplier of Goods/Services (Service Provider) shall submit a copy of the 'Government Notification' to evidence the rate as applicable on the Bid due date and on the date of revision.

21. Beyond the contract period, in case OIL is not entitled for input tax credit of GST, then any increase in the rate of GST beyond the contractual delivery period shall be to Service provider's account whereas any decrease in the rate GST shall be passed on to the OIL.

22. Beyond the contract period, in case OIL is entitled for input tax credit of GST, then statutory variation in applicable GST on supply and on incidental services, shall be to OIL's account.

23. Claim for payment of GST/Statutory variation, should be raised within two [02] months from the date of issue of 'Government Notification' for payment of differential (in %) GST, otherwise claim in respect of above shall not be entertained for payment of arrears.

24. The base date for the purpose of applying statutory variation shall be the Bid Opening Date.

25. The contractor will be liable to ensure to have registered with the respective tax authorities, wherever applicable and to submit self-attested copy of such registration certificate(s) and the Contractor will be responsible for procurement of material in its own registration (GSTIN) and also to issue its own Road Permit/ E-way Bill, if applicable etc.

26. In case the bidder is covered under Composition Scheme under GST laws, then bidder should quote the price inclusive of the GST (CGST & SGST/UTGST or

IGST). Further, such bidder should mention "Cover under composition system" in column for GST (CGST & SGST/UTGST or IGST) of price schedule.

27. OIL will prefer to deal with registered supplier of goods/services under GST. Therefore, bidders are requested to get themselves registered under GST, if not registered yet. However, in case any unregistered bidder is submitting their bid, their prices will be loaded with applicable GST while evaluation of bid. Where OIL is entitled for input credit of GST, the same will be considered for evaluation of bid as per evaluation methodology of tender document.

28. Procurement of Specific Goods: Earlier, there is no tax incidence in case of import of specified goods (i.e. the goods covered under List-34 of Customs Notification no. 12/2012-Cus dated. 17.03.2012 as amended). Customs duty is not payable as per the policy. However, under GST regime, IGST Plus GST compensation cess (if applicable) would be leviable on such imports. Bidders should quote GST as inclusive considering IGST component for the imported Materials portion while quoting their prices on destination basis. However, GST rate to be specified in the price bid format.

29. Documentation requirement for GST

i. The Contractor will be under the obligation for invoicing correct tax rate of tax/duties as prescribed under the GST law to OIL, and pass on the benefits, if any, after availing input tax credit.
ii. Any invoice issued shall contain the following particulars:
iii. Name, address and GSTIN of the supplier;
iv. Serial number of the invoice;
v. Date of issue;
vi. Name, address and GSTIN or UIN, if registered of the recipient;
vii. Name and address of the recipient and the address of the delivery, along with the State and its code,
viii. HSN code of goods or Accounting Code of services[SAC];
ix. Description of goods or services;
x. Quantity in case of goods and unit or Unique Quantity Code thereof;
xi. Total value of supply of goods or services or both;
xii. Taxable value of supply of goods or services or both taking into discount or abatement if any;
xiii. Rate of tax (IGST,CGST, SGST/UTGST, cess);
xiv. Amount of tax charged in respect of taxable goods or services (IGST,CGST, SGST/UTGST, cess);
xv. Place of supply along with the name of State, in case of supply in the course of interstate trade or commerce;
xvi. Address of the delivery where the same is different from the place of supply and
xvii. Signature or digital signature of the supplier or his authorised representative.
xviii. GST invoice shall be prepared in triplicate, in case of supply of goods, in the following manner:
The original copy being marked as ORIGINAL FOR RECIPIENT;
The duplicate copy being marked as DUPLICATE FOR TRANSPORTER and
The triplicate copy being marked as TRIPLICATE FOR SUPPLIER.

In case of any advance given against any supplies contract, the supplier of the goods shall issue Receipt Voucher containing the details of details of advance taken along with particulars as mentioned in clause no. (a), (b), (c), (d), (g), (k), (l), (m) & (o) above.

30. **Anti-profiteering clause**

As per Clause 171 of GST Act it is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit to the consumer by way of commensurate reduction in prices. The Supplier of Goods/Services may note the above and quote their prices accordingly.

31. In case the GST rating of Contractor on the GST portal/Govt. official website is negative/black listed, then the bids may be rejected by OIL. Further, in case rating of bidder is negative/black listed after award of work for supply of goods/services, then OIL shall not be obligated or liable to pay or reimburse GST to such Contractor and shall also be entitled to deduct/recover such GST along with all penalties/interest, if any, incurred by OIL.

15.0 CONFIDENTIALITY AGREEMENT:

OIL Confidentiality and Non-Disclosure Agreement (NDA) shall be applicable, and bidder has to submit Non-Disclosure Agreement as per given format in NIT duly signed & sealed by the authorized signatory of the bidder, along with the bid.

Notes:

- **HEADINGS:** The headings of the clauses of the contract are for convenience only and shall not be used to interpret the provisions thereof.
- Company hereby acknowledges that the equipment and tools ("Equipment") that are owned and utilized by Contractor to perform its service obligations under the Contract shall be at all times be, handled and manned by the Contractor. Company shall not be entitled to use/operate/possess any of the Contractor's Equipment for providing Services under the Contract. To clarify that control, custody and possession of Contractor's equipment shall always be with the Contractor.
- All the clauses in this tender are limited to execution of this tender only and do not carry any precedence whatsoever for any OIL's such or similar tenders in future.

End of STC

SECTION-III

SCOPE OF WORK (SOW) REVISED

1.0 INTRODUCTION

Oil India Limited (OIL), a national oil company in India under the control of the Ministry of Petroleum and Natural Gas, is involved in the exploration, development, production of crude oil and natural gas, transportation of crude oil, and production of LPG. The company makes extensive use of Information and Communication Technology (ICT) and Operational Technology (OT) in its operations. To ensure the security of its ICT and OT systems, OIL is seeking the services of a Cybersecurity Consultancy firm (referred hereafter as the CONSULTANT/VENDOR/BIDDER).

The consultant shall be tasked with conducting an assessment and review of OIL's existing ICT and OT systems, identifying and analyzing cybersecurity risks, redesigning systems for mitigation, formulating relevant policies and procedures, defining the organizational unit responsible for cybersecurity, building the IT, OT, and cybersecurity governance structure, and training stakeholders on the project outcomes.

2.0 SCOPE OF WORK

The goal of this project is to establish a comprehensive cybersecurity program throughout the organization, making use of personnel, processes, and technologies to construct a strong and secure ICT and OT infrastructure for Oil India Limited.

The project shall be executed in the following stages:

Stage-1: As-Is Assessment

1. Technology assessment for ICT infrastructure
2. Technology assessment for OT infrastructure
3. Cybersecurity governance assessment
4. Cybersecurity risk assessment
5. Vulnerability assessment, penetration testing and application security assessment for ICT infrastructure

Stage-2: Development of the Cybersecurity Program

1. Development of target state architecture and gap assessment
2. Development of cybersecurity governance and organization structure
3. Formulation of policies, processes and procedures

Stage-3: Development of the Action Plan

1. Identification and prioritization of opportunities for improvement (OFI)
2. Development of action plan
3. Development of functional and technical specifications for the identified OFIs along with implementation plan

Stage-4: Communication to Stakeholders and Project Closure

1. Workshop and presentation to the management
2. Awareness training to the core team members
3. Acceptance and project closure

3.0 PROJECT EXECUTION

3.1 Project Team Composition

3.1.1 Structure

The structure of the Project Team is defined below:

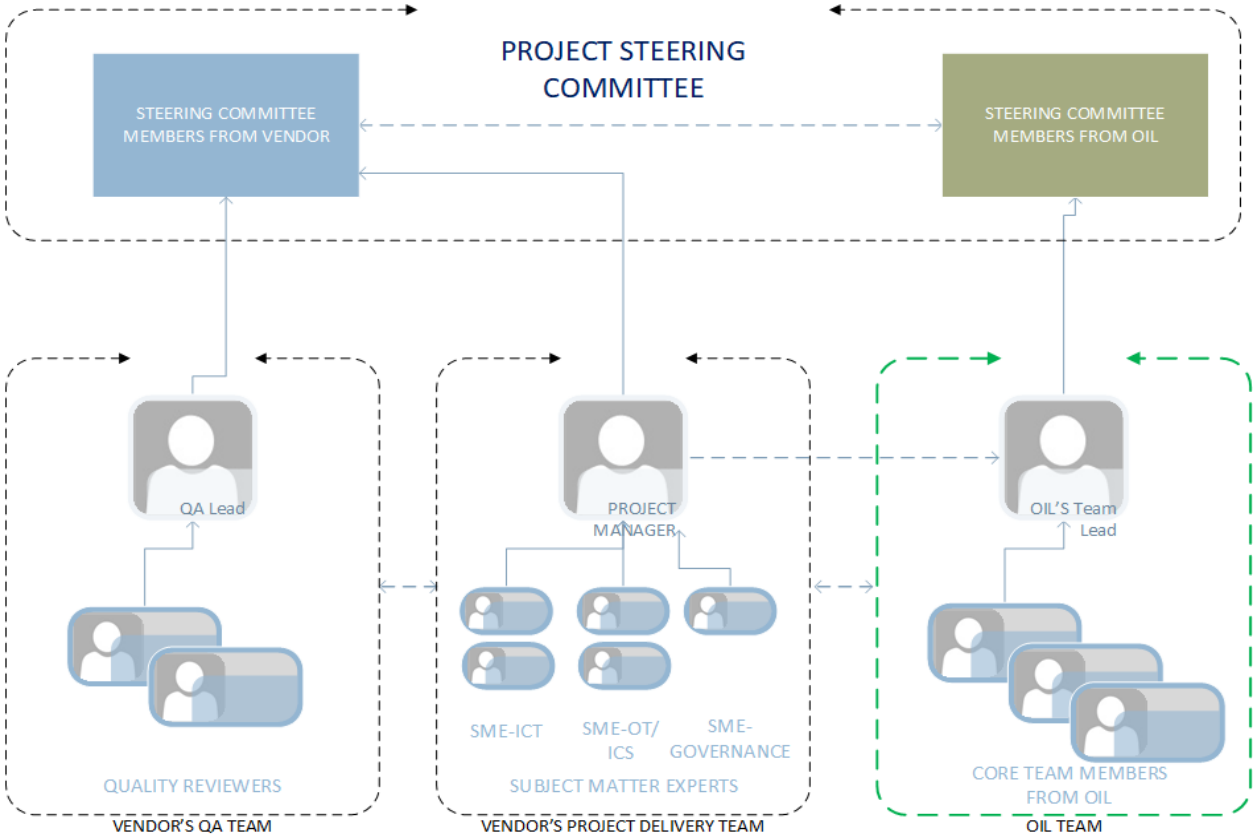


Figure 1: Project Team Structure

1. The **Project Steering Committee** shall be responsible for making key decisions, signing off major deliverables and has the overall responsibility for execution of the project. This committee shall constitute senior members from both the Consultant's organization and OIL.

2. The Consultant's **Project Delivery Team** shall be responsible for carrying out the project activities and shall consist of relevant subject matter experts led by the **Project Manager**.

3. The Consultant shall constitute a team independent from the Project Delivery Team for quality assurance (QA) of the project deliverables. This team shall be responsible for quality review of the project deliverables before delivery to OIL. The QA team is not required to be present onsite at the OIL's location.

4. OIL shall constitute a **Core Team** with members from relevant functions, which shall engage with the Project Delivery Team for different project activities. The Core Team shall be led by **OIL's Team Lead**.

3.1.2 **Human Resources**

I) **Acceptable Industry Certificates**

Following is the list of acceptable industry certificates for various roles in the project.

Pool-1	1. Certified Information Systems Auditor (CISA) 2. Certified Information Security Manager (CISM) 3. Certified Information Systems Security Professional (CISSP) 4. Certification in Risk and Information Systems Control (CRISC) 5. Certified Chief Information Security Officer (CCISO)
Pool-2	1. Offensive Security Certified Professional (OSCP) 2. Certified Network Defender (CND) 3. CCIE – Routing and Switching or equivalent OEM certificate from other networking vendors. 4. CCIE – Security or equivalent OEM certificate from other networking vendors 5. MCSE: Core Infrastructure 6. GIAC Certified Enterprise Defender (GCED) 7. Certified Information Systems Security Professional (CISSP) 8. Open Group Certified Architect 9. Certified Information Privacy Professional (CIPP) 10. Certified Data Privacy Solutions Engineer (CDPSE) 11. CCSK (Certificate of Cloud Security Knowledge) 12. AWS Certified Security – Specialty 13. Microsoft Certified: Azure Security Engineer Associate 14. Certified Cloud Security Professional (CCSP)

	15. Google Cloud Certified - Professional Cloud Security Engineer 16. CEH
Pool-3	1. ISA/IEC 62443 Cybersecurity Expert (ICE) 2. ISA/IEC 62443 Cybersecurity Fundamentals Specialist 3. ISA/IEC 62443 Cybersecurity Risk Assessment Specialist 4. ISA/IEC 62443 Cybersecurity Design Specialist 5. GIAC Industrial Cybersecurity Certification (GICSP) 6. Certified SCADA Security Architect (CSSA) 7. Global Industrial Cybersecurity Professional (GICSP)
Pool-4	1. ISO/IEC 27001:2013 Information security management system lead auditor 2. Post Graduate Diploma in Cyber Law of minimum one-year duration. 3. CEH
Note: 1. For any of the certificates listed above, higher level certificate in the same certification track shall also be acceptable. For example, Offensive Security Certified Expert (OSCE) is acceptable in lieu of Offensive Security Certified Professional (OSCP). 2. The certificates must be valid as on bid closing date.	

Table 1: Acceptable Industry Certificates

II) **Consultant's Steering Committee Member**

The Consultant shall deploy their representative(s) on the Steering Committee. The Consultant is permitted to deploy additional manpower as per their requirement.

Role	**Minimum Count**	
Member of Steering Committee	1	The Member of Steering Committee who qualifies as per BEC/BRC Clause No. 4.0 A) shall have the followings: 1. In-depth knowledge of cybersecurity concepts, frameworks, standards such as NIST, ISO, and IEC. 2. Hands-on experience in conducting cybersecurity assessments for critical infrastructure or industrial control systems. 3. Hands-on experience in Cybersecurity Transformation projects. Note: Relevant documents confirming to the above must be submitted along with the technical bid.

III) **Project Delivery Team**

The Consultant shall deploy a project delivery team for execution of the project. The Consultant is permitted to deploy additional manpower as per requirement.

Role	**Minimum Count**	
Project Manager	1	The Project Manager who qualifies as per BEC/BRC Clause No. 4.0 B) shall have the followings: 1. In-depth knowledge of cybersecurity concepts, frameworks, and standards such as NIST, ISO, and IEC. 2. Hands-on experience in conducting cybersecurity assessments for critical infrastructure or industrial control systems. Note: Relevant documents confirming to the above must be submitted along with the technical bid.
Subject Matter Expert – ICT Security	2	The Subject Matter Experts qualifying as per BEC/BRC Clause No. 4.0 B) shall have the followings: Out of the minimum 02 members, at least 01 member should have experience in the following fields: a) Active Directory Security Assessment b) Security assessment for Microsoft 365 platform c) Cloud security d) Network Architecture Design e) Network Security f) Zero Trust g) Application Security h) Data Protection i) Security Operations Note: Relevant documents confirming to the above must be submitted along with the technical bid.
Subject Matter Expert – OT/ICS Security	2	The Subject Matter Experts qualifying as per BEC/BRC Clause No. 4.0 B) shall have the followings: Out of the minimum 02 members, at least 01 member should have experience in the following fields: a. Design and development of Industrial Automation/Industrial Control Systems.

Role	Minimum Count	
		b. Implementation of security controls for Industrial Automation/Industrial Control Systems. Note: Relevant documents confirming to the above must be submitted along with the technical bid.
Subject Matter Expert – Cybersecurity Governance	1	The Subject Matter Expert - Cybersecurity Governance qualifying as per BEC/BRC Clause No. 4.0 B) shall have the followings: 1. A thorough understanding of various regulations and standards related to cybersecurity such as NIST, ISO, COBIT, IT Act 2000 of India etc. 2. Cyber laws. Note: Relevant documents confirming to the above must be submitted along with the technical bid.

IV) **Quality Assurance Team**

The Consultant shall deploy a Quality Assurance Team for quality review of the project deliverables. The Consultant is permitted to deploy additional manpower as per requirement. This team must be independent from the Steering Committee members and Project Delivery team.

Role	Minimum Count	Experience
QA Lead	1	The Quality Assurance Team qualifying as per BEC/BRC Clause No. 4.0 C) shall have the followings: 1. In-depth knowledge of cybersecurity concepts, frameworks, standards such as NIST, ISO, and IEC. 2. Hands-on experience in conducting cybersecurity assessments for critical infrastructure or industrial control systems. Note: Relevant documents confirming to the above must be submitted along with the technical bid.
Quality Reviewer	2	

V) **Project Governance**

1. A formal communication protocol shall be established between the Consultant and OIL as per the following schedule for activity status updates:

Frequency	**Meeting/Reporting Type**	**Purpose**	**Attendees**
Weekly	Weekly Status Update Report	To provide an update on the activities performed and any interim observations	• Consultant's Project Manager • Consultant's Project Delivery Team • OIL Core Team
Monthly	Monthly Status Update Report	To provide a monthly update on activities performed	• Steering Committee members • Consultant's Project Delivery Team • OIL Core Team and relevant person
Ad-hoc	As needed/via email or in person	To communicate roadblocks and potential high-risk items	• Consultant's Project Manager • Consultant's Project Delivery Team • OIL Core Team

Table 2: Communication Protocol

2. All project documentation deliverables must undergo version control processes. Every document must be reviewed by the QA team of the Consultant before delivery to OIL.

3. All project deliverables must be signed off by the Consultant's representative on the Steering Committee before final delivery to OIL.

4. The Consultant shall record Minutes of meeting (MoM) to record the discussions, decisions, and actions taken during a meeting or interview with OIL's teams.

5. The Consultant shall initiate the project by arranging a project kickoff meeting. The project kickoff meeting shall be attended by the project steering committee members along with the Consultant's project delivery team and OIL's core team.

6. The Consultant shall submit a detailed project plan to OIL as per the timeline mentioned in Clause No. 9.0 of SCC. The project plan must contain the following details:

a. **Project Schedule**: Details on activities and dependency relationship along with corresponding Gantt chart.

b. **Human resource details and roles and responsibilities**: Roles and responsibilities of all team members should be clearly defined and communicated.

c. **Communication plan**: Communication methods and frequency should be established to ensure effective communication throughout the project.

d. **Approval Process**: An approval process should be defined for all project deliverables to ensure that they meet the requirements and are approved by the appropriate stakeholders.

e. **Risk Management**: Project risks should be identified, analyzed, and mitigated as necessary to minimize potential impact on the project.

7.0 REFERENCE STANDARDS AND FRAMEWORKS

The Consultant shall have to design the cybersecurity program for OIL in compliance with the following global standards and frameworks:

1. ISO/IEC TS 27110:2021 - Information technology, cybersecurity, and privacy protection — Cybersecurity framework development guidelines

2. ISO/IEC 27001:2022 - Information security, cybersecurity, and privacy protection — Information security management systems — Requirements

3. ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements

4. NIST Cybersecurity Framework

5. NIST: Framework for improving Critical Infrastructure Cybersecurity

6. NIST: SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security

7. ISA/IEC 62443

8. Cybersecurity Capability Maturity Model (C2M2) published by DOE, U.S. [C2M2 Model]

5.0 COMPLIANCE TO LEGAL AND GOVERNMENT GUIDELINES

The consultant shall ensure that cybersecurity program designed for OIL complies with the Information Technology Act, 2000 of India and its subsequent amendments and

applicable guidelines and advisories issued by the relevant Government of India ministries and agencies like MeitY, CERT-In, NCIIPC etc.

6.0 CYBERSECURITY CONSTITUENCY

In the context of this tender, the cybersecurity constituency refers to the defined group of users, locations, information and communication technology/operational technology assets, cloud assets, data resident on ICT/OT/cloud assets, networks, and units/entities/functions within OIL that are directly or indirectly impacted by cybersecurity concerns.

The proposed Cybersecurity Program for OIL shall cover this entire cybersecurity constituency. The following sections give indicative (but not exhaustive) details on the cybersecurity constituency.

6.1 Users

There are around 7000 users who use OIL's information and communication technology services internally. Additionally, there are about 3500 endpoint computers in operation within the organization.

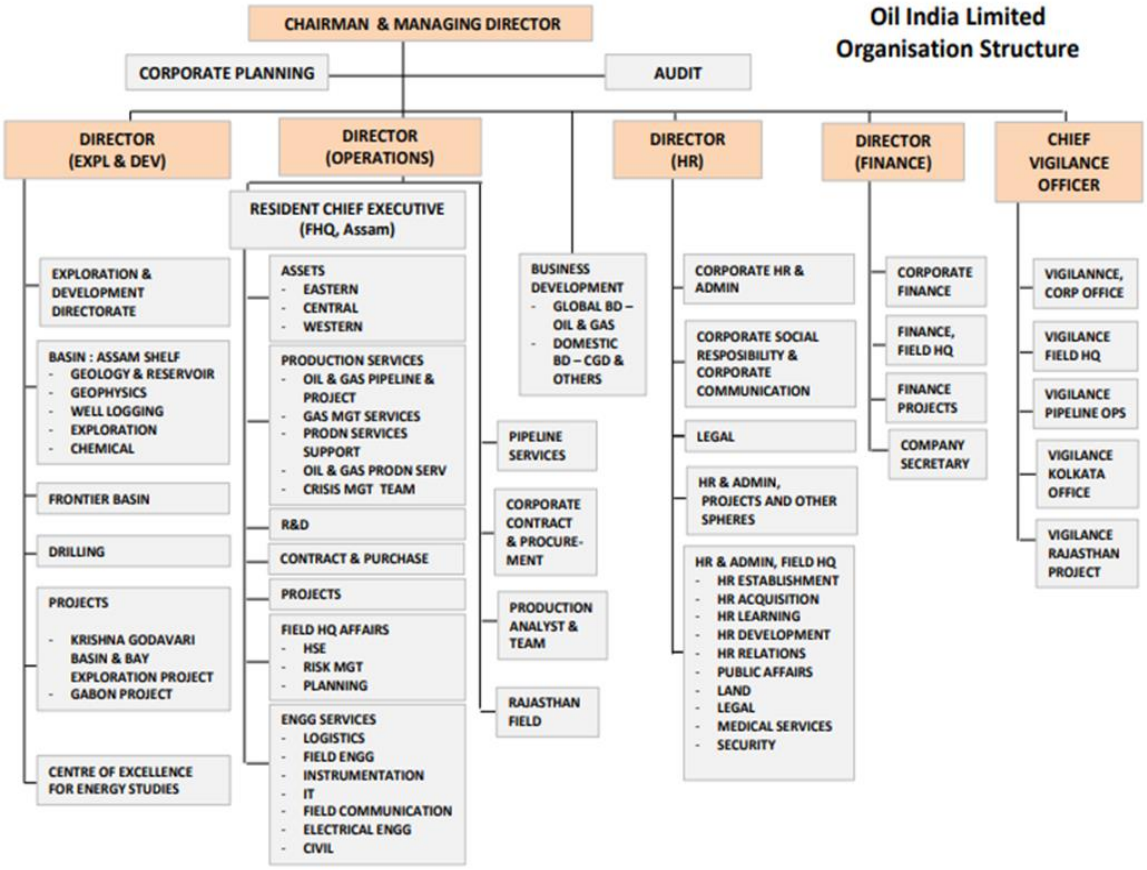
6.2 About the Company

6.2.1 Major Business Processes

Following are the key business processes at OIL:

1. Exploration of Hydrocarbons
2. Production of Crude Oil and Natural Gas
3. Transportation of crude oil and petroleum products
4. LPG Production
5. IT Business Processes

6.2.2 The following is the organization chart of OIL:



6.2.3 Locations and Org Units

In India, OIL has offices in the following locations:

Corporate HQ	Noida, UP
Registered Office and Field HQ	Duliajan, Assam
Moran Oil Field	Moran, Assam
Eastern Producing Area	Digboi, Assam
Pipeline Headquarters	Guwahati, Assam
CoEES	Guwahati, Assam
Delhi Office	New Delhi
Kolkata Branch	Kolkata, West Bengal
Kolkata Shipping Office	Kolkata, West Bengal
Mahanadi Basin Project	Bhubaneswar, Odisha
Kakinada Office	Kakinada, Andhra Pradesh
Rajasthan Field	Jodhpur, Rajasthan

Table 3: List of locations

OIL has ~60 Org Units/Departments across all the above locations.

6.3 ICT Assets

The following units/entities/functions within OIL uses ICT for various business functions:

Information Technology
ERP
Geology and Reservoir
Geophysics
Drilling
Production
Well Logging
Civil Engineering
Security
HR
Legal
Land
Health and Safety
Planning
Pipeline
Oil, Gas Pipeline & Projects
Projects
Field Communication

Table 4: ICT Assets

6.4 Cloud Assets

OIL makes use of public cloud infrastructure (IaaS, PaaS) hosted by MeitY empaneled Cloud Service Providers for some of its business applications.

6.5 Network

OIL has established a comprehensive data network connection that spans across all its offices and utilizes a combination of Gigabit LAN, wireless networks, radio connectivity, and VSAT. The inter-office connection is established through MPLS connectivity, and each office has its own local Internet connection.

The following table gives indicative list of installed network devices:

Network Devices		
	Internal Firewalls	6
	Firewalls	22
	Routers	50
	Switches	250

Table 5: List of Network Devices

6.6 OT Assets

The following units/entities/functions within OIL uses OT for various business functions:

Pipeline	• Crude oil pipeline • Product Pipeline
Gas Management Services	• Gas Compressor Stations • Gas Gathering Stations
Production Support Services	• Tank Farms
LPG	• LPG Recovery Plant • LPG Bottling Plant
Electrical	• Power Plant
Instrumentation	• DCS, PLC and various SCADA systems at field locations
Drilling	• Rig locations

Table 6: List of OT Assets

6.7 Functions

The following functions within OIL are directly impacted by Cybersecurity risks to ICT and OT assets.

Business Process	**Function**
Information Technology	IT
Enterprise resource planning (ERP)	ERP
Finance and Accounting	F&A
Exploration	Geology and Reservoir
	Geophysics
	Well-logging
Communications	FC
	Pipeline Telecom

Production & Processing of Crude Oil & Gas	SCADA systems at FHQ
	SCADA systems at Rajasthan
	Drilling Operations – DCS/PLC systems
	STF
	CGGS
Pipeline	Crude and Product Pipeline Operations
LPG Plant	LPG
HR	HR Group
Land Acquisition	Land
Legal & Compliance	Legal
Engineering Services	Civil Engineering
	Electrical
Projects	Projects

Table 7: List of Functions

Here "function" also refers to the part of the organization that is being evaluated based on the C2M2 model.

6.8 **Web & Mobile Application**

1. Total number of Applications: 40
2. Total No. of Mobile applications: 10

7.0 **DETAILED SCOPE OF WORK**

7.1 **STAGE-1: AS-IS ASSESSMENT**

The purpose of the as-is assessment is to provide a clear and accurate understanding of the current situation, without making any assumptions or modifications.

In the context of cybersecurity, the as-is assessment shall be used to evaluate OIL's current cybersecurity posture, including its policies, procedures, technology, and risk management practices. The assessment shall identify strengths and weaknesses in the current cybersecurity framework and provide a baseline for future improvement efforts.

7.1.1 Pre-Requisites

The following table defines the list of pre-requisites for commencement of activities in this stage.

SL.NO.	Description
1.	The project kick-off meeting was held with participation from key stakeholders from both OIL and the Consultant.
2.	Project plan reviewed and approved by OIL
3.	Team member composition of the delivery team responsible for this stage is approved by OIL
4.	Signing of NDA by each member of the delivery team

Table 8:Stage-1 Pre-requisites

7.1.2 Methodology

The Consultant shall adopt the following assessment methodology for carrying out the AS-IS assessment:

1. The Consultant shall conduct the independent activities concurrently as much as possible, for example, different teams may perform assessments for separate functions at the same time.

2. The team of consultants responsible for carrying out the assessment activities shall visit all the locations of OIL as specified in [6.2] for the assessment exercise. The consultants shall be onsite at OIL's offices for the entire duration of this stage.

3. For the critical functions mentioned in [0], the consultants shall conduct C2M2 [8] self-evaluation workshops with the appropriate attendees.

4. The consultants shall conduct interview-based discussions with the respective stakeholders.

5. The consultants shall review the existing policies and procedures and relevant records.

6. The consultants shall collect all relevant information like past audits, incident reports etc.

7. The consultant is permitted to deploy and utilize necessary software tools for conducting assessments, given that they do not interfere with production environments, with prior approval from OIL. Such tools should not require significant changes to the OIL's systems and processes.

8. The AS-IS assessment shall be done with reference to the NIST CSF Version 1.1, and the current cybersecurity posture shall be identified as the "Current Profile". The "Current Profile" shall be developed for each of the individual functions of OIL.

7.1.3 List of Activities

The following activities shall be performed in this stage:

7.1.3.1 Technology Assessment for ICT infrastructure

1. Discovery of ICT assets and preparation of updated Asset Register with inventory of
   a. Physical devices and systems
   b. Software platforms and applications
   c. Organizational communication and data flow
   d. External Information systems
   e. Suppliers and third-party partners of information systems, components, and services

2. Review of Endpoint security with emphasis on
   a. Endpoint protection mechanisms
   b. Unauthorized access to cloud resources
   c. Unauthorized remote access
   d. Patch management
   e. Endpoint management tool being used
   f. Review of EDR policies

3. Review of Network architecture and Network Security with emphasis on
   a. Network segmentation
   b. Network Access Control
   c. Connectivity of the corporate network with any public network
   d. Connectivity of the corporate network with any OT network
   e. Wireless network access
   f. OIL's ICT services accessible from public Internet
   g. Review of Firewall configuration and applied policies

4. Review of Software patch management processes and current status

5. Review of application development practices (application code review is outside the scope of the project)

   a. Development, testing and production environments.
   b. Version control system
   c. Secure programming practices

6. Review of ICT assets on Public Cloud with emphasis on
   a. Operation and Maintenance and Administration practices
   b. Network connectivity with OIL corporate network
   c. Network connectivity with public network

7. Security assessment for Microsoft 365 platform – configuration review of the existing Microsoft 365 tenant security configuration for OIL

8. Active Directory Security Assessment (ADSA) with emphasis on
   a. Review of operational processes
   b. Review of the privileged accounts/groups membership as well as regular account hygiene
   c. Review of the forest and domain trusts
   d. Review operating system configuration, security patch, and update levels
   e. Review of domain and domain controller configuration compared to Microsoft recommended guidance.
   f. Review of key Active Directory object permission delegation

9. Review of installed security solutions and controls
   a. Review of Firewall configuration and applied policies
   b. Review of physical security and access control

10. Review of Infrastructure security – DHCP, DNS, NTP

11. Review controls related to Data security.

12. Review of controls related to removable media.

13. Review of Identity and Access Management

14. Review of Privilege Identity and Access Management

15. Review of Remote Access/Teleworking provisions and MDM practices

16. Review of Remote maintenance practices for ICT assets

17. Review of User Awareness and Training practices

18. Review of configuration management of critical infrastructure

19. Review Backup and Recovery practices

20. Review of Vulnerability management practices

21. Review of Database security
22. Discovery of shadow IT - the unauthorized use of any digital service or device that is not formally approved of and supported by the IT department.

23. Review of Log management and event data collection practices for monitoring and detection of potential cyber threats

24. Supply Chain and vendor services review

25. Identification of critical ICT services for continuity of business operations of OIL

26. Identification of dependencies and critical functions for delivery of critical ICT services

27. Identification of Resilience requirements to support delivery of critical ICT services for all operating states (e.g., under duress/attack, during recovery, normal operations)

7.1.3.2 Technology Assessment for OT infrastructure

1. Discovery of OT assets and preparation of updated Asset Register with inventory of

    a. Physical devices and systems
    b. Software platforms and applications
    c. Organizational communication and data flow
    d. External Information systems
    e. Suppliers and third-party partners of the OT systems, components, and services

2. Review of Network Architecture for OT systems with emphasis on

    a. Connectivity to OIL corporate network
    b. Connectivity to any public network – Internet exposure discovery
    c. Connectivity with the field equipment
    d. Remote connectivity
    e. Existing Security Controls

3. Review of installed security solutions and controls
    a. Review of Firewall configuration and applied policies
    b. Review of physical security and access control

4. Review of endpoint security

5. Review of Software patch management processes and current status

6. Review controls related to Data security.

7. Review of controls related to removable media.
8. Review of Remote Access/Teleworking provisions

9. Review of Remote maintenance practices for OT assets

10. Review of Privilege and Identity Access Management

11. Review of User Awareness and Training practices

12. Review of configuration management of critical infrastructure

13. Review Backup and Recovery practices

14. Review of Vulnerability management practices

15. Configuration review of OT systems, operations and controls

16. Review of Log management and event data collection practices for monitoring and detection of potential cyber threats

17. Supply Chain and vendor services review

18. Identification of critical OT services for continuity of business operations of OIL

19. Identification of dependencies and critical functions for delivery of critical OT services

20. Identification of Resilience requirements to support delivery of critical OT services for all operating states (e.g., under duress/attack, during recovery, normal operations)

7.1.3.3 Vulnerability assessment (VA), Penetration testing (PT) and application security assessment for both ICT and OT infrastructure

1. OSINT (Open-Source Intelligence) Vulnerability Discovery: Identification of vulnerabilities in ICT and OT infrastructure of OIL by collecting and analyzing publicly available information. This information can come from a variety of sources, including social media, forums, blogs, news websites, and other publicly available databases.

2. Both External and Internal VA&PT exercises involving Reconnaissance, Scanning, Vulnerability Analysis, non-destructive Exploitation and Post-Exploitation analysis. (Approx. count of external IPs: 50, Approx. count of internal IPs: 250 to 300. The count mentioned here is an approximate/indicative figure only. The bidder has to discover the exact count during the Stage-1 of the SOW).

3. Web and Mobile application VA&PT (including minimum OWASP Top 10 risks).

4. If it is deemed that performing penetration testing on certain systems may cause disruptions in the production environment, OIL reserves the right to exclude those systems from the scope of the testing exercise.

5. The method of Vulnerability assessment (VA), Penetration testing (PT) and application security will preferably be grey box.

7.1.3.4 Cybersecurity Governance assessment

Cybersecurity governance assessment shall be used to evaluate OIL's governance framework for managing cybersecurity risks. The objective of this assessment is to identify areas for improvement in the governance framework and make recommendations for enhancing the effectiveness of the governance process.
This assessment shall cover the following:

1. Review of existing cybersecurity policies and procedures w.r.t ICT and OT systems of OIL

2. Review of existing cybersecurity governance mechanisms including cybersecurity roles and responsibilities and authority, identification of allied disciplines, and roles and responsibilities of key stakeholders.

3. Assessment of risk management processes

4. Evaluation of incident response and management practices

5. Evaluation of compliance with relevant regulations and standards, prevalent cyber laws, reviewing OIL's compliance with relevant regulations and standards related to cybersecurity.

6. Evaluation of training and awareness programs

7.1.3.5 Cybersecurity Risk Assessment

The cybersecurity risk assessment exercise shall be used to identify, assess, and prioritize the risks that OIL faces from various cybersecurity threats.

The assessment shall cover the following:

1. **Identification of critical ICT and OT assets** which are critical for business continuity of OIL.

2. Threat identification: This involves identifying the types of threats that OIL is most likely to face for its critical ICT and OT assets.

3. **Impact analysis**: This involves assessing the potential impact of each identified threat and vulnerability, including the potential harm to sensitive information, financial losses, and disruption to business operations.

4. **Risk calculation and prioritization**: This involves calculating the overall risk level for each threat and vulnerability, considering the likelihood of occurrence and the potential impact.

5. Development of risk mitigation plan

6. **Recommendations for mitigation**: This involves making recommendations for reducing the risks associated with each threat and vulnerability.

7.1.4 Deliverables

The following table defines the deliverables for Stage-1: As-Is assessment.

Given that the target audience for each assessment topic shall vary, each topic shall be presented in a separate document. And it is also expected that the processes and maturity levels across different locations, organizational units, and functions shall vary. As a result, each document shall include separate sections for different locations, organizational units, functions, etc.

If the bidder determines that an additional document is necessary, they may submit one.

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
1.	Asset Register (ICT)	ICT-ASSET-REGISTER	Encrypted PDF	[1]
2.	Assessment Report on Endpoint Security (ICT)	ICT-ASSESSMENT-REPORT-ENDPOINT	Encrypted PDF	[2]
3.	Assessment Report on Network Infrastructure (ICT)	ICT-ASSESSMENT-REPORT-NETWORK	Encrypted PDF	[3], [10]
4.	Assessment Report on Software Patch Management (ICT)	ICT-ASSESSMENT-REPORT-PATCH	Encrypted PDF	[4]
5.	Assessment Report on Application Development & Database Security (ICT)	ICT-ASSESSMENT-REPORT-APP-DEV	Encrypted PDF	[5], [21]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
6.	Assessment Report on Cloud Security (ICT)	ICT-ASSESSMENT-REPORT-CLOUD	Encrypted PDF	[6]
7.	Security Assessment Report on MS365 (ICT)	ICT-ASSESSMENT-REPORT-MS365	Encrypted PDF	[7]
8.	Active Directory Security Assessment Report (ICT)	ICT-ASSESSMENT-REPORT-ADSA	Encrypted PDF	[8]
9.	Assessment Report on Existing Security Controls (ICT)	ICT-ASSESSMENT-REPORT-CONTROLS	Encrypted PDF	[9]
10.	Assessment Report on Data Security (ICT)	ICT-ASSESSMENT-REPORT-DATA-SEC	Encrypted PDF	[11], [12]
11.	Assessment Report on IAM (ICT)	ICT-ASSESSMENT-REPORT-IAM	Encrypted PDF	[13], [14]
12.	Assessment Report on Remote Access (ICT)	ICT-ASSESSMENT-REPORT-REMOTE-ACCESS	Encrypted PDF	[15], [16]
13.	Assessment Report on User Awareness (ICT)	ICT-ASSESSMENT-REPORT-USER-AWARENESS	Encrypted PDF	[17]
14.	Assessment Report on Configuration Management (ICT)	ICT-ASSESSMENT-REPORT-CONFIG-MGMT	Encrypted PDF	[18]
15.	Assessment Report on Backup Management (ICT)	ICT-ASSESSMENT-REPORT-BACKUP	Encrypted PDF	[19]
16.	Assessment Report on Vulnerability Management (ICT)	ICT-ASSESSMENT-REPORT-VM	Encrypted PDF	[20]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
17.	Discovery Report on Shadow IT	ICT-ASSESSMENT-REPORT-SHADOW-IT	Encrypted PDF	[22]
18.	Assessment Report on Log Management and Monitoring (ICT)	ICT-ASSESSMENT-REPORT-LOG-MONITORING	Encrypted PDF	[23]
19.	Assessment Report on Supply Chain and Vendor Management (ICT)	ICT-ASSESSMENT-REPORT-VENDOR	Encrypted PDF	[24]
20.	Assessment Report on Critical ICT services	ICT-ASSESSMENT-REPORT-CRITICAL-ICT	Encrypted PDF	[25], [26], [27]
21.	Asset Register (OT)	OT-ASSET-REGISTER	Encrypted PDF	[1]
22.	Assessment Report on Network Infrastructure (OT)	OT-ASSESSMENT-REPORT-NETWORK	Encrypted PDF	[2]
23.	Assessment Report on Existing Security Controls (OT)	OT-ASSESSMENT-REPORT-CONTROLS	Encrypted PDF	[3]
24.	Assessment Report on Endpoint Security (OT)	OT-ASSESSMENT-REPORT-ENDPOINT	Encrypted PDF	[4]
25.	Assessment Report on Software Patch Management (OT)	OT-ASSESSMENT-REPORT-PATCH	Encrypted PDF	[5]
26.	Assessment Report on Data Security (OT)	OT-ASSESSMENT-REPORT-DATA-SEC	Encrypted PDF	[6], [7]
27.	Assessment Report on Remote Access (OT)	OT-ASSESSMENT-REPORT-	Encrypted PDF	[8], [9]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
		REMOTE-ACCESS		
28.	Assessment Report on IAM (OT)	OT-ASSESSMENT-REPORT-IAM	Encrypted PDF	[10]
29.	Assessment Report on User Awareness (OT)	OT-ASSESSMENT-REPORT-USER-AWARENESS	Encrypted PDF	[11]
30.	Assessment Report on Configuration Management (OT)	OT-ASSESSMENT-REPORT-CONFIG-MGMT	Encrypted PDF	[12]
31.	Assessment Report on Backup Management (OT)	OT-ASSESSMENT-REPORT-BACKUP	Encrypted PDF	[13]
32.	Assessment Report on Vulnerability Management (OT)	OT-ASSESSMENT-REPORT-VM	Encrypted PDF	[14]
33.	Assessment Report on Current Configuration (OT)	OT-ASSESSMENT-REPORT-CONFIGURATION	Encrypted PDF	[15]
34.	Assessment Report on Log Management and Monitoring (OT)	OT-ASSESSMENT-REPORT-LOG-MONITORING	Encrypted PDF	[16]
35.	Assessment Report on Supply Chain and Vendor Management (OT)	OT-ASSESSMENT-REPORT-VENDOR	Encrypted PDF	[17]
36.	Assessment Report on Critical OT services	OT-ASSESSMENT-REPORT-CRITICAL-ICT	Encrypted PDF	[18], [19], [20]
37.	OS-INT Report on ICT Infra	ICT-ASSESSMENT-REPORT-OSINT	Encrypted PDF	[1]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
38.	OS-INT Report on OT Infra	OT-ASSESSMENT-REPORT-OSINT	Encrypted PDF	[1]
39.	VA-PT Report on ICT Infra	ICT-ASSESSMENT-REPORT-VA-PT	Encrypted PDF	[2], [3]
40.	VA-PT Report on OT Infra	OT-ASSESSMENT-REPORT-VA-PT	Encrypted PDF	[2], [3]
41.	Assessment Report on Cybersecurity Governance	ICT-OT-ASSSESSMENT-REPORT-GOVERNANCE	Encrypted PDF	[7.1.3.4]
42.	Critical Asset Register (ICT)	ICT-CRITICAL-ASSET-REGISTER	Encrypted PDF	[1]
43.	Critical Asset Register (OT)	OT-CRITICAL-ASSET-REGISTER	Encrypted PDF	[1]
44.	Cybersecurity Risk Assessment Report	ICT-OT-ASSSESSMENT-REPORT-RISK	Encrypted PDF	[7.1.3.5]
45.	C2M2 Self-evaluation Reports for each of the function defined in [0]	C2M2-SELF-EVALUATION-REPORT-<function-name>	Encrypted PDF	[3]
46.	Executive Summary Report for Stage-1	STAGE-1-EXECUTIVE-SUMMARY	Encrypted PDF	A brief, concise summary of the Stage-1 Deliverables providing a high-level understanding.
47.	Phase wrap-up presentation	STAGE-1-WRAP-UP-REPORT	Presentation over virtual meeting, Encrypted PDF of the Presentation slides	The phase wrap presentation shall include information about the objectives and goals of this stage, the tasks that

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
				were completed and the results achieved, any challenges or obstacles that were encountered, and the impact of the stage on the overall project. It may also include a discussion of the lessons learned, the next steps, and any changes to the project plan.

Table 9: Stage-1 Deliverables

7.1.5 Stage Conclusion Checklist

The table below outlines the criteria for determining the successful completion of this stage. All items on the checklist must be fully completed by the Consultant before submitting the invoice for payment corresponding to this stage.

SL.NO.	Description	Reference
1.	Fulfilment of the pre-requisite conditions specified in 7.1.1	[7.1.1]
2.	Visit of delivery team to all locations completed	[2]
3.	Onsite presence of the Project Delivery Team responsible for this stage for entire duration of the stage.	[2]
4.	C2M2 Self-evaluation workshops for all functions completed	[3]
5.	Interview based discussion held with the persons responsible for each function	[4]
6.	Existing policies and procedures, past audits and incidents reviewed	[5]
7.	Final version of all the deliverables defined in 7.1.4 received and approved by OIL	[7.1.4]

Table 10: Stage-1 Conclusion Checklist

7.2 STAGE-2: DEVELOPMENT OF THE CYBERSECURITY PROGRAM

7.2.1 Pre-Requisites

The following table defines the list of pre-requisites for commencement of activities in this stage.

SL.NO.	Description
1.	Team member composition of the delivery team responsible for this stage is approved by OIL
2.	Signing of NDA by each member of the delivery team
3.	Stage-1 Conclusion Checklist complete

Table 11: Stage 2 Pre-requisites

7.2.2 Methodology

1. To create a target profile as per the NIST Cybersecurity Framework (CSF), the following steps should be followed:

    a. **Review the NIST CSF**: The Consultant shall thoroughly review the NIST CSF Version 1.1 and familiarize themselves with its categories and subcategories.
    b. **Assess Business Needs**: The Consultant shall assess OIL's business needs and requirements to determine which NIST CSF categories and subcategories are most relevant to their operations.
    c. **Use the Risk Assessment findings from Stage-1**: The Consultant shall use the risk assessment findings to identify the current state of cybersecurity posture for OIL and determine the potential risks that need to be addressed.
    d. **Identify Priority Areas**: Based on the review of NIST CSF and the result of the business needs assessment and risk assessment, the Consultant shall identify the categories and subcategories that are the highest priority for OIL to focus on.
    e. **Develop the Target Profile**: Using the priority areas identified, the Consultant shall develop the target profile for OIL. The target profile should describe the desired "to-be" state of cybersecurity for OIL and outline the specific steps that need to be taken to achieve it.

2. After creating the target profile according to the NIST CSF, the Consultant shall then evaluate the differences between the current profile and the target profile. Based on this evaluation, the Consultant shall design a target state architecture that addresses these differences and aims to bring the current profile closer to the target profile. This will involve modifications to policies, processes, procedures, organizational structure, governance, and technology infrastructure.

3. The consultants assigned to perform the tasks in this phase shall be physically present in the OIL office in Duliajan for at least 5 days during the assigned timeframe for this stage. This allows for direct interaction and discussions with the relevant OIL teams.

7.2.3 List of Activities

The following activities shall be performed in this stage:

7.2.3.1 Development of Cybersecurity Governance and Organization Structure

1. Definition of cybersecurity roles and responsibilities and authority.
2. Definition of the organization structure, charter, and mission statement for the organization unit in OIL responsible for the overall cybersecurity function.

3. Establishing a Cybersecurity governance framework that defines the decision-making processes, roles, and responsibilities for managing Cybersecurity risks.

4. Establishing clear lines of communication and decision-making processes for Cybersecurity incidents.

5. Identification of allied disciplines ensure that all relevant areas and stakeholders are considered and included in the cybersecurity program to provide a more comprehensive and integrated approach to managing cybersecurity risks and ensuring the security of the organization's assets and operations.

7.2.3.2 Formulation of Policies, Processes and Procedures

The security requirements for ICT and OT systems can be different and therefore it is important to have separate policies that cater to the specific needs of each of these systems. The policies should address the specific security challenges and risks associated with each system and ensure that appropriate security measures are in place to protect the assets and information.

1. Development of organizational information security policies covering at-least the following areas for both ICT and OT systems:

   a. Information security/Cybersecurity policy
   b. Acceptable Use Policy
   c. Disaster recovery policy
   d. Incident Response Policy
   e. Mobile device security policy
   f. Network security policy
   g. Network Segmentation Policy
   h. Identity and Access Management policy
   i. Remote access policy

j. Risk management policy
k. Security awareness and training policy
l. Third-party security policy
m. Vulnerability management policy
n. Data Classification Policy
o. Data protection policy
p. Endpoint Security Policy
q. Data Backup and Recovery Policy
r. Change Management Policy
s. Security Monitoring Policy
t. Asset Management Policy
u. 3rd Party Information Exchange Policy
v. Access Control Policy
w. Patch Management Policy
x. Configuration Management Policy
y. Cloud security Policy
z. Software Development Policy

2. Development of Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) including Cyber Crisis Management Plan

3. Development of Processes and Standard Operating Procedures (SOP) aligned with the respective ICT/OT security policies.

7.2.3.3 Development of Target State Architecture for Technology Infrastructure

Development of Design & Architecture for target state covering the following areas in both ICT and OT Technology Infrastructure:

1. Network Architecture and Network Security
2. Endpoint Security
3. Zero Trust principle
4. Backup and business continuity
5. Identity and Access management
6. Secure adoption of Cloud services
7. Secure Application Development
8. Monitoring and Detection
9. Infrastructure components – Active Directory/AAA systems, DNS and DHCP
10. Data Protection
11. Access Control
12. Resilience and Availability

7.2.4 Deliverables

The following table defines the deliverables for Stage-2.

If the vendor determines that an additional document is necessary, they may submit one.

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
1.	OIL's Cybersecurity Governance and Organization structure	GOVERNANCE-ORG-STRUCTURE	Encrypted PDF	[7.2.3.1]
2.	Information security /Cybersecurity policy for ICT assets	ICT-POL-SECURITY	Encrypted PDF	[1.a]
3.	Acceptable Use Policy for ICT assets	ICT-POL-ACCEPTABLE-USAGE	Encrypted PDF	[1.b]
4.	Disaster Recovery Policy for ICT assets	ICT-POL-DR	Encrypted PDF	[1.c]
5.	Incident Response Policy for ICT assets	ICT-POL-IR	Encrypted PDF	[1.d]
6.	Mobile Device Security Policy for ICT assets	ICT-POL-MD	Encrypted PDF	[1.e]
7.	Network Security Policy for ICT assets	ICT-POL-NW-SEC	Encrypted PDF	[1.f]
8.	Network Segmentation Policy for ICT assets	ICT-POL-NW-SEG	Encrypted PDF	[1.g]
9.	IAM Policy for ICT assets	ICT-POL-IAM	Encrypted PDF	[1.h]
10.	Remote Access Policy for ICT assets	ICT-POL-REMOTE	Encrypted PDF	[1.i]
11.	Risk Management Policy for ICT assets	ICT-POL-RM	Encrypted PDF	[1.j]
12.	Security Awareness and Training Policy for ICT assets	ICT-POL-TRG	Encrypted PDF	[1.k]
13.	Third Party Security Policy for ICT assets	ICT-POL-3RD-PARTY	Encrypted PDF	[1.l]
14.	Vulnerability Management Policy for ICT assets	ICT-POL-VM	Encrypted PDF	[1.m]
15.	Data Classification Policy for ICT assets	ICT-POL-DATA-CLASS	Encrypted PDF	[1.n]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
16.	Data Protection Policy for ICT assets	ICT-POL-DATA-PROTECT	Encrypted PDF	[1.o]
17.	Endpoint Security Policy for ICT assets	ICT-POL-ENDPOINT	Encrypted PDF	[1.p]
18.	Data Backup and Recovery Policy for ICT assets	ICT-POL-DATA-BACKUP	Encrypted PDF	[1.q]
19.	Change Management Policy for ICT assets	ICT-POL-CM	Encrypted PDF	[1.r]
20.	Security Monitoring Policy for ICT assets	ICT-POL-MONITORING	Encrypted PDF	[1.s]
21.	Asset Management Policy for ICT assets	ICT-POL-ASSET	Encrypted PDF	[1.t]
22.	Third Party Information Exchange Policy for ICT assets	ICT-POL-3RD-INFO-EXCHANGE	Encrypted PDF	[1.u]
23.	Access Control Policy for ICT assets	ICT-POL-ACCESS-CTRL	Encrypted PDF	[1.v]
24.	Patch Management Policy for ICT assets	ICT-POL-PATCH	Encrypted PDF	[1.w]
25.	Configuration Management Policy for ICT assets	ICT-POL-CM	Encrypted PDF	[1.x]
26.	Cloud Security Policy for ICT assets	ICT-POL-CLOUD	Encrypted PDF	[1.y]
27.	Software Development Policy for ICT assets	ICT-POL-SW-DEV	Encrypted PDF	[1.z]
28.	Information security /Cybersecurity policy for OT assets	OT-POL-SECURITY	Encrypted PDF	[1.a]
29.	Acceptable Use Policy for OT assets	OT-POL-ACCEPTABLE-USAGE	Encrypted PDF	[1.b]
30.	Disaster Recovery Policy for OT assets	OT-POL-DR	Encrypted PDF	[1.c]
31.	Incident Response Policy for OT assets	OT-POL-IR	Encrypted PDF	[1.d]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
32.	Mobile Device Security Policy for OT assets	OT-POL-MD	Encrypted PDF	[1.e]
33.	Network Security Policy for OT assets	OT-POL-NW-SEC	Encrypted PDF	[1.f]
34.	Network Segmentation Policy for OT assets	OT-POL-NW-SEG	Encrypted PDF	[1.g]
35.	IAM Policy for OT assets	OT-POL-IAM	Encrypted PDF	[1.h]
36.	Remote Access Policy for OT assets	OT-POL-REMOTE	Encrypted PDF	[1.i]
37.	Risk Management Policy for OT assets	OT-POL-RM	Encrypted PDF	[1.j]
38.	Security Awareness and Training Policy for OT assets	OT-POL-TRG	Encrypted PDF	[1.k]
39.	Third Party Security Policy for OT assets	OT-POL-3RD-PARTY	Encrypted PDF	[1.l]
40.	Vulnerability Management Policy for OT assets	OT-POL-VM	Encrypted PDF	[1.m]
41.	Data Classification Policy for OT assets	OT-POL-DATA-CLASS	Encrypted PDF	[1.n]
42.	Data Protection Policy for OT assets	OT-POL-DATA-PROTECT	Encrypted PDF	[1.o]
43.	Endpoint Security Policy for OT assets	OT-POL-ENDPOINT	Encrypted PDF	[1.p]
44.	Data Backup and Recovery Policy for OT assets	OT-POL-DATA-BACKUP	Encrypted PDF	[1.q]
45.	Change Management Policy for OT assets	OT-POL-CM	Encrypted PDF	[1.r]
46.	Security Monitoring Policy for OT assets	OT-POL-MONITORING	Encrypted PDF	[1.s]
47.	Asset Management Policy for OT assets	OT-POL-ASSET	Encrypted PDF	[1.t]
48.	Third Party Information Exchange Policy for OT assets	OT-POL-3RD-INFO-EXCHANGE	Encrypted PDF	[1.u]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
49.	Access Control Policy for OT assets	OT-POL-ACCESS-CTRL	Encrypted PDF	[1.v]
50.	Patch Management Policy for OT assets	OT-POL-PATCH	Encrypted PDF	[1.w]
51.	Configuration Management Policy for OT assets	OT-POL-CM	Encrypted PDF	[1.x]
52.	Cloud Security Policy for OT assets	OT-POL-CLOUD	Encrypted PDF	[1.y]
53.	Software Development Policy for OT assets	OT-POL-SW-DEV	Encrypted PDF	[1.z]
54.	Incident Response and Business Continuity plan	ICT-OT-IR-BCP-PLAN	Encrypted PDF	[2]
55.	Incident Recovery and Disaster Recovery plan	ICT-OT-IR-DR-PLAN	Encrypted PDF	[2]
56.	Cyber Crisis Management Plan	ICT-OT-CCMP	Encrypted PDF	[2]
57.	Target State Architecture Document for Network Architecture and Network Security (ICT)	ICT-ARCH-NW	Encrypted PDF	[1]
58.	Target State Architecture Document for Endpoint Security (ICT)	ICT-ARCH-ENDPOINT	Encrypted PDF	[2]
59.	Target State Architecture Document for ZTP (ICT)	ICT-ARCH-ZTP	Encrypted PDF	[3]
60.	Target State Architecture Document for Backup and BC (ICT)	ICT-ARCH-BACKUP	Encrypted PDF	[4]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
61.	Target State Architecture Document for IAM (ICT)	ICT-ARCH-IAM	Encrypted PDF	[5]
62.	Target State Architecture Document for Cloud Adoption (ICT)	ICT-ARCH-CLOUD	Encrypted PDF	[6]
63.	Target State Architecture Document for Secure Application Development (ICT)	ICT-ARCH-SW-DEV	Encrypted PDF	[7]
64.	Target State Architecture Document for Monitoring and Detection (ICT)	ICT-ARCH-MONITORING	Encrypted PDF	[8]
65.	Target State Architecture for Infra Components (ICT)	ICT-ARCH-INFRA	Encrypted PDF	[9]
66.	Target State Architecture for Data Protection	ICT-ARCH-DATA-PROTECTION	Encrypted PDF	[10]
67.	Target State Architecture for Access Control	ICT-ARCH-ACCESS-CONTROL	Encrypted PDF	[11]
68.	Target State Architecture for Resiliency and Availability (ICT)	ICT-ARCH-HA	Encrypted PDF	[12]
69.	Target State Architecture Document for Network Architecture and Network Security (OT)	OT-ARCH-NW	Encrypted PDF	[1]
70.	Target State Architecture Document for	OT-ARCH-ENDPOINT	Encrypted PDF	[2]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
	Endpoint Security (OT)			
71.	Target State Architecture Document for ZTP (OT)	OT-ARCH-ZTP	Encrypted PDF	[3]
72.	Target State Architecture Document for Backup and BC (OT)	OT-ARCH-BACKUP	Encrypted PDF	[4]
73.	Target State Architecture Document for IAM (OT)	OT-ARCH-IAM	Encrypted PDF	[5]
74.	Target State Architecture Document for Cloud Adoption (OT)	OT-ARCH-CLOUD	Encrypted PDF	[6]
75.	Target State Architecture Document for Secure Application Development (OT)	OT-ARCH-SW-DEV	Encrypted PDF	[7]
76.	Target State Architecture Document for Monitoring and Detection (OT)	OT-ARCH-MONITORING	Encrypted PDF	[8]
77.	Target State Architecture for Infra Components (OT)	OT-ARCH-INFRA	Encrypted PDF	[9]
78.	Target State Architecture for Data Protection	OT-ARCH-DATA-PROTECTION	Encrypted PDF	[10]
79.	Target State Architecture for Access Control	OT-ARCH-ACCESS-CONTROL	Encrypted PDF	[11]
80.	Target State Architecture for Resiliency and Availability (OT)	OT-ARCH-HA	Encrypted PDF	[12]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
81.	Executive Summary Report for Stage-2	STAGE-2-EXECUTIVE-SUMMARY	Encrypted PDF	A brief, concise summary of the Stage-2 Deliverables providing a high-level understanding.
82.	Phase wrap-up presentation	STAGE-2-WRAP-UP-REPORT	Presentation over virtual meeting, Encrypted PDF of the Presentation slides	The phase wrap presentation shall include information about the objectives and goals of this stage, the tasks that were completed and the results achieved, any challenges or obstacles that were encountered, and the impact of the stage on the overall project. It may also include a discussion of the lessons learned, the next steps, and any changes to the project plan.

Table 12: Stage-2 Deliverables

7.2.5 Stage Conclusion Checklist

The table below outlines the criteria for determining the successful completion of this stage. All items on the checklist must be fully completed by the vendor before submitting the invoice for payment corresponding to this stage.

SL.NO.	Description	Reference
1.	Fulfilment of the pre-requisite conditions specified in [7.2.1]	[7.2.1]
2.	Onsite presence of the Project Delivery Team responsible for this stage for at least 5 days	[3]

SL.NO.	Description	Reference
3.	Final version of all the deliverables defined in [7.2.4] received and approved by OIL	[7.2.4]

Table 13: Stage 2 Conclusion Checklist

7.3 STAGE-3: DEVELOPMENT OF THE ACTION PLAN

7.3.1 Pre-Requisites

The following table defines the list of pre-requisites for commencement of activities in this stage.

SL.NO.	Description
4.	Team member composition of the delivery team responsible for this stage is approved by OIL
5.	Signing of NDA by each member of the delivery team
6.	Stage-2 Conclusion Checklist complete

Table 14: Stage 3 Pre-requisites

7.3.2 Methodology

In this stage, the consultant shall develop the Action Plan for implementation of the Cybersecurity Program developed in Stage-2 of the project.

The action plan shall include (among others) the following:

1. List of all Opportunities for Improvement (OFI), for bridging the gap between "Current" and "Target" profiles.
2. Prioritization and classification of the OFIs based on mutual discussions with OIL.
3. Roadmap of specific steps, resources, and timelines required to implement each OFI.
4. Functional and Technical specifications for the High Priority OFIs.
5. Budget, personnel, technology and prospective vendors/service providers required to support the high priority OFI outlined in the action plan.

The consultants assigned to perform the tasks in this phase shall be physically present in the OIL office in Duliajan for at least 10 days during the assigned timeframe for this stage. This allows for direct interaction and discussions with the relevant OIL teams.

7.3.3 List of Activities

The following activities shall be performed in this stage:

7.3.3.1

Identification and prioritization of Opportunities for Improvement (OFI)

1. Identification of all OFIs for bridging the gap between "Current" and "Target" profiles.

2. Prioritization of the OFIs based on the following criteria (among others):
    a. Risk
    b. Urgency
    c. Benefit
    d. Feasibility
    e. Cost
    f. Complexity
    g. Dependency on other OFIs

3. Further clarification of the OFIs into the following two categories:

a. **Tactical**: Short-term, immediate actions and decisions which are simple to implement, requiring minimal investments, but with potential to positively impact the security posture of OIL.

b. **Strategic**: Long-term, actions and decisions which are complex to implement, may require substantive investments and resources, but with a significant impact on the overall cybersecurity program of OIL.

7.3.3.2

Development of Action Plan

1. Development of a detailed Action Plan for adoption and implementation of the Cybersecurity Program for OIL with the following details:

a. Goals and Objectives
b. Identified gaps between the "Current" and "Target" profiles and the corresponding OFIs
c. Detailed recommendations for each OFI
d. Prioritized action plan with tasks, scope, timeline and responsibilities
e. Necessary resources including budget, personnel and technology

2. Amongst the prioritized OFIs, OIL will select ten (10) tactical and five (5) strategic OFI for immediate action.

7.3.3.3

Development of Functional and Technical Specifications for the selected OFIs

For each of the fifteen (15) selected OFIs in [2], the vendor will prepare detailed Functional and technical specifications with details on:

1. Scope of work
2. Project implementation plan
3. Budget and resource requirements

7.3.4 Deliverables

The following table defines the deliverables for Stage-3.
If the vendor determines that an additional document is necessary, they may submit one.

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
1.	List of all identified, prioritized and classified OFIs	LIST-OF-OFI	Encrypted PDF	[1], [2], [3]
2.	Action Plan	ACTION-PLAN	Encrypted PDF	[1]
3.	Functional and Technical Spec for selected OFIs	FS-TACTICAL-OFI-01 FS-TACTICAL-OFI-02 FS-TACTICAL-OFI-03 FS-TACTICAL-OFI-04 FS-TACTICAL-OFI-05 FS-TACTICAL-OFI-06 FS-TACTICAL-OFI-07 FS-TACTICAL-OFI-08 FS-TACTICAL-OFI-09 FS-TACTICAL-OFI-10 FS-STRATEGIC-OFI-01 FS-STRATEGIC-OFI-02 FS-STRATEGIC-OFI-03 FS-STRATEGIC-OFI-04 FS-STRATEGIC-OFI-05		[7.3.3.3]
4.	Executive Summary Report for Stage-3	STAGE-3-EXECUTIVE-SUMMARY	Encrypted PDF	A brief, concise summary of the Stage-3 Deliverables providing a high-level understanding.
5.	Phase wrap-up presentation	STAGE-3-WRAP-UP-REPORT	Presentation over virtual meeting,	The phase wrap presentation shall include information about the objectives

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
			Encrypted PDF of the Presentation slides	and goals of this stage, the tasks that were completed and the results achieved, any challenges or obstacles that were encountered, and the impact of the stage on the overall project. It may also include a discussion of the lessons learned, the next steps, and any changes to the project plan.

Table 15: Stage-3 Deliverables

7.3.5 Stage Conclusion Checklist

The table below outlines the criteria for determining the successful completion of this stage. All items on the checklist must be fully completed by the vendor before submitting the invoice for payment corresponding to this stage.

SL.NO.	Description	Reference
1.	Fulfilment of the pre-requisite conditions specified in [7.3.1]	[7.3.1]
2.	Onsite presence of the Project Delivery Team responsible for this stage for at least 10 days	[7.3.2]
3.	Final version of all the deliverables defined in [7.3.4] received and approved by OIL	[7.3.4]

Table 16: Stage 3 Conclusion Checklist

7.4 STAGE-4: COMMUNICATION TO STAKEHOLDERS AND PROJECT CLOSURE

7.4.1 Pre-Requisites

The following table defines the list of pre-requisites for commencement of activities in this stage.

SL.NO.	Description
1.	Team member composition of the delivery team responsible for this stage is approved by OIL
2.	Signing of NDA by each member of the delivery team
3.	Stage-3 Conclusion Checklist complete

Table 17: Stage 4 Pre-requisites

7.4.2 Methodology

During the final stage of the project, various communication methods such as workshops, presentations, and awareness training will be employed to inform OIL's management and relevant teams about the project outcome, aiming to obtain their agreement and alignment with the OIL's Cybersecurity Program. Additionally, the vendor will provide the final set of documents required for the project closure.

7.4.3 List of Activities

The following activities shall be performed in this stage:

7.4.3.1 Workshop and Presentation to the Management

The vendor is responsible for conducting the following workshops and presentations:

1. A workshop for top management:

   a. This workshop will be conducted for the Top management of OIL, to convey the strategic level vision and roadmap for implementation of OIL's cybersecurity program. The presentations will cover executive summary of the project journey, its findings and outcomes.
   b. The workshop is required to be held in person at OIL's Corporate Headquarters in Noida, and the Program Management Team consisting of members from both OIL and the vendor must be physically present at the workshop.
   c. The workshop will not exceed the duration of one day.

2. A workshop for function heads and other relevant key personnel.

   a. This workshop will be conducted for the function heads and other relevant key personnel of OIL, to convey the strategic as well as operational/tactical level vision and roadmap for implementation of OIL's cybersecurity program. The presentations will cover executive summary of the project journey, its findings and outcomes along with the action plan.
   b. The workshop is required to be held in person at OIL's Field Headquarters in Duliajan, and the Program Management Team consisting of members from both OIL and the vendor must be physically present at the workshop.
   c. The workshop will not exceed the duration of one day.

7.4.3.2 Awareness training to the Core Team Members

For each of the functions defined in [0], individual awareness training sessions shall be held for the relevant Core Team members.

1. The awareness sessions will be held via virtual meetings with the relevant core team members of OIL.
2. The awareness sessions will not exceed a duration of 3 hours each.
3. The awareness sessions will be conducted through customized presentations for each function, focusing on the current and target profiles, action plan, and roadmap for implementing the cybersecurity program.

7.4.3.3 Acceptance and Project Closure Report

The project closure activity, which will mark the acceptance of the project, is the final step in the project. As part of this activity, the vendor will provide the following documents:

1. **Project Completion report**: This document provides an overview of the project objectives, scope, outcomes, deliverables, and any issues or challenges that arose during the project.

2. **Project Closure checklist**: This document outlines all the final status of all the tasks required to officially close the project in accordance with the tender.

7.4.4 Deliverables

The following table defines the deliverables for Stage-4.

If the vendor determines that an additional document is necessary, they may submit one.

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
1.	Workshop for the Top Management	WORKSHOP-SLIDES-TOP-MGMT	In person presentation Encrypted PDF of the presentation slides and copy of any other materials	[1]

SL.NO.	DESCRIPTION	DOCUMENT ID	DOCUMENT FORMAT	Reference to addressable areas
			provided to the attendees	
2.	Workshop for the function heads and other relevant key personnel	WORKSHOP-SLIDES-FUNCTION-HEAD	In person presentation Encrypted PDF of the presentation slides and copy of any other materials provided to the attendees	[2]
3.	Awareness training to the Core Team Members for each function listed in []	TRG-SLIDES--<function-name>	Presentation over virtual meeting Encrypted PDF of the presentation slides and copy of any other materials provided to the attendees	[7.4.3.2]
4.	Project Completion report	PROJECT-COMPLETION-REPORT	Encrypted PDF	[1]
5.	Project Closure checklist	PROJECT-CLOSURE-CHECKLIST	Encrypted PDF	[2]

Table 18: Stage 4 Deliverables

7.4.5 Stage Conclusion Checklist

The table below outlines the criteria for determining the successful completion of this stage. All items on the checklist must be fully completed by the vendor before submitting the invoice for payment corresponding to this stage.

SL.NO.	Description	Reference
1.	Fulfilment of the pre-requisite conditions specified in [7.4.1]	[7.4.1]
2.	Final version of all the deliverables defined in [7.4.4] received and approved by OIL	[7.4.4]

Table 19: Stage 4 Conclusion Checklist

8.0 SPECIAL TERMS

1. The bidder must fill up and submit the bidder's technical Response Sheet as specified in Annexure-C along with the bid. **The information provided in this document shall be used for the technical scrutiny of the tender.**

2. The bidder must submit an **Approach Paper** along with their offer for executing the project including the following details:

a. Understanding of OIL's requirement
   - Scope of work
   - Deliverables
   - Global standards/frameworks to be used as reference.

b. Technical Approach and Methodology for Delivery of Cybersecurity Program
c. Tools and automation enablers to be used.
d. Pre-requisites for OIL
e. Delivery Plan and Team Composition
   - Delivery Plan and Staffing Schedule for various stages of Cybersecurity Program.
   - Team composition with details of industry certificates, qualifications, and work experience.
   - Project Governance
   - Roles and Responsibilities

3. Post submission of the bid, the bidder shall give a technical presentation covering the details included in the Approach Paper to OIL.

End of SOW