RFP Ref. No.: GSTN/P&C/CISO/CI/08-2025/P-12 Date: 04/09/2025

GOODS AND SERVICES TAX NETWORK

REQUEST FOR PROPOSAL FOR RENEWAL OF CYBER-RISK INSURANCE POLICY OF GSTN

GOODS AND SERVICES TAX NETWORK (GSTN)
4th Floor, East Wing, World Mark-1, Aerocity, New Delhi – 110037
Tel: 011-49111200
Website: www.gstn.org.in

Disclaimers and Disclosures

Goods And Services Tax Network (GSTN) has prepared this document to give background information to interested parties for participating in this RFP/Tender. While GSTN has taken due care in the preparation of this RFP/Tender document and believes it to be accurate, neither GSTN nor any of its authorities or agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it. The information is not intended to be exhaustive.

Interested bidders/agencies/parties are required to make their own inquiries and respondents will be required to confirm in writing that they have done so, and they do not rely only on the information provided by GSTN in submitting a bid. The information is provided on the basis that it is non–binding on GSTN or any of its authorities or agencies or any of their respective officers, employees, agents or advisors. GSTN reserves the right to modify the requirements as well as add or delete, as the case may be, to meet GSTN's requirements at any point of time.

GSTN reserves the right not to proceed with the RFP/Tender, to alter the Key details reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the matter further with any bidder/agency/party expressing interest.

GSTN reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever. GSTN does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the tender without assigning any reason whatsoever. GSTN also has the right to re-issue the tender without the Bidder having the right to object to such reissue.

This RFP is neither an offer from GSTN nor does it constitute any binding obligation or commitment on GSTN. This RFP is only a document that invites interested agencies/parties to, on a non-exclusive basis, express an interest with no obligation, commitment or liability of any manner devolving on GSTN, either on account of the issue of this RFP/Tender to the interested agencies/parties, or upon receipt of any response from the interested agencies/parties thereto, or any meetings or presentations made.

No reimbursement of cost of any type will be paid to persons or entities expressing interest. All expenses incurred by the interested parties as a result of responding to, or further to this RFP/Tender, are to their own account and GSTN will not be liable in this respect whatsoever. No reimbursement of cost of any type will be paid to persons or entities proposing a solution. Please note that any part or the whole of information, directly or indirectly learnt, for any other purpose, other than for conducting work under the ambit of the RFP/Tender issued by GSTN is not authorized.

Table of Contents

Acronyms

Acronym	Description
EMD	Earnest Money Deposit
GCC	General Conditions of Contract
GIB	General Instructions to Bidders
GST	Goods And Services Tax
GSTN	Goods And Services Tax Network (Organization)
LD	Liquidated Damages
LOA / PO	Letter of Award / Purchase Order
LOI	Letter of Intent
OIC	Officer In-Charge
PBG	Performance Bank Guarantee
PQ	Pre-Qualification Criteria
QCBS	Quality and Cost Base Selection
RFP	Request for Proposal
SCC	Special Conditions of Contract
SIB	Special Instructions to Bidders
TBA	To be announced

SECTION - I

Key Details

RFP reference No.	GSTN/P&C/CISO/CI/08-2025/P-12
RFP Details	**Request for Proposal for Renewal of Cyber-Risk Insurance Policy of GSTN**
Last date & time for submission of Bid	**25th September, 2025 at 15.00 hrs**
Pre-bid Meeting details	**10th September, 2025 at 11.30 hrs.** at GSTN office Note: Clarifications to be submitted by **08th September, 2025 till 15.00 hrs** as per format in **Annexure-V** in excel format through e-mail only. Queries submitted after stated deadline shall not be considered. To attend pre-bid meeting at GSTN office, the representatives (02 Nos.) of bidders are requested to carry their company I-card/ Authorization letter (on Company's letter head). Without Company I-Card/Authorization letter, no bidder will be allowed to attend the Prebid/bid opening meeting.
Place of Bid opening	Goods And Services Tax Network "East wing, 4th floor, World Mark -1, Aerocity, New Delhi - 110037.
Bid Opening details **(Technical Bid)**	Bids shall be Opened on **25th September, 2025 at 15.30 hrs** at GSTN office.
Opening of **Financial bids**	The date of opening of financial bids will be informed separately to successful Insurance brokers/bidders after technical evaluation of bids and only those bids will be opened which are technically qualified.
Earnest Money Deposit (EMD)	**NIL**
Method of Selection	The method of selection is Quality and Cost Base Selection **(QCBS).** The weights given to the Technical and Commercial Bids are: **Technical = 70%** and **Commercial = 30%**
Envelope details	Bid shall consist of 02 envelopes containing following: **Envelope-I (PART-A)** Response to Eligibility criterion and Technical Qualification criterion with supporting documents. **Envelope-II (PART-B)** Financial Proposal only. All the Two envelopes should be sealed in another envelope and indicating Tender Number, Subject, Bid Opening Date and Time
Address for communication	**The VP (Procurement & Contracts)** Goods And Services Tax Network "East wing, 4th floor, World Mark -1, Aerocity, Delhi – 110 037 **Email:** anirudh.rawat@gstn.org.in sanjaysharma.pc@gstn.org.in **Phone no.:** 011-49111200 (Ext. 347)

Notice Inviting Proposal

To,

Sub: **Invitation of sealed Proposal for "Renewal of Cyber-Risk Insurance Policy of GSTN".**

1. Goods and Services Tax Network (GSTN) is a Section 8 company (under The Companies Act 2013). The Company has been set up primarily to provide IT infrastructure and services to the Central and State Governments, tax payers and other stakeholders for implementation of the Goods and Services Tax (GST).

2. Goods and Services Tax Network (GSTN) invites sealed bids from eligible Empanelled Insurance Brokers for the 'RFP for renewal of Cyber-Risk Insurance Policy of GSTN' covering all its projects/platforms (e.g. GST System, E-Way Bill, E-invoice System etc.), operations, systems and GST network.

3. Bidders mean Insurance Companies (Insurers) who will submit their bids through GSTN empaneled insurance brokers/advisors for getting quotes/bids from insurance companies on behalf of GSTN.

4. Empanelled Insurance Brokers shall ensure that their bids, complete in all respects, are submitted on or before the closing date and time indicated in the key details, failing which the bids will be treated as late and rejected.

5. In the event of any of the above-mentioned dates being declared as a holiday / closed day for the purchase organization, the bids will be received/opened on the next working day at the appointed time.

6. The Bid shall be deemed to have been submitted after careful study and examination of the RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Incomplete or non-responsive bids shall be rejected. Also, the grounds for rejection of Bid should not be questioned after the final declaration of the successful Bidder.

7. The content of this RFP is copyright material of Goods and Services Tax Network (GSTN). No part or material of this RFP document should be published in paper or electronic media without prior written permission from GSTN.

8. RFP shall mean Request for Quotation. Bid, Tender, RFP and RFQ are used to mean the same.

9. Bidder should seek necessary clarifications by e-mail as mentioned in Key Details, if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document.

10. All entries in the Bid form should be legible and filled clearly. Any overwriting or correction which is unavoidable has to be signed by the authorized signatory.

11. Each page of the proposal should be sequentially numbered, signed, and stamped by the authorized signatory as a token of acceptance of the terms and conditions laid down by GSTN in this RFP.

12. GSTN takes no responsibility for delay, loss or non-receipt of bid documents sent by post either way. Bids should be submitted in physical (hardcopy) form, bids received through e-mail shall not be considered.

13. Only such bids which are received through the empanelled insurance brokers will be entertained. An insurer will be allowed to submit a bid only through one of the GSTN's empanelled insurance broker agency. Any submission otherwise made will be rejected out rightly.

14. GSTN reserves the right to accept or reject any or all of the bids in full or in part including the lowest bid without assigning any reasons or incurring any liability thereof.

For **Goods And Services Tax Network**

Sanjay Sharma
Vice President (P&C)

SECTION-II: SCOPE OF WORK

1. Scope of work/coverage and nature of cover:

It is intended to have a cyber insurance policy to cover first-party loss and third-party liability coverage to organization when cyber-risk materializes and/or cyber security controls at organization fails.

The Risk details are represented below:

Type	Cyber Liability Insurance
Insured	Goods and Services Tax Network (GSTN)
Business	Design, Develop, Implement and manage the goods and services tax platform across the country
Cover trigger	Claims Made Basis
Policy period	**From: 13.10.2025** **To : 12.10.2026** **Both days inclusive**
Limit of Indemnity	INR **100 Crores** per claim and in aggregate
Territorial limit	Worldwide including USA/Canada
Law & jurisdiction	Worldwide including USA/Canada
Deductible	**Not more than Rs. 50 lakhs** **Time deductible is not more than 12 hours**
Insurance to cover both First party and third party liabilities, as applicable, for scope of cover/ extensions, without any sub-limits unless otherwise specified.	
Scope of cover/extensions	• Ransomware attack, Cyber extortion, cyber terrorism coverage etc. full limit • Security breach and/or Privacy Breach • Hacking / data theft Cover, Denial of service (DDOS) attacks: Rs.35 Lakh • Cover for Network Security claims and Network Access liability including liability arising from insertion of any malicious code/or virus/Trojan horse, worm or logic bomb/malware attack/Conduit Liability/ Impaired access liability • Cover for PII/SPI and the Data managed by GSTN

	• Cover for Disclosure/Data Privacy Liability including but not limited to virus/malware attack, introduction of malicious code or unauthorized access leading to data breach • Data recovery expenses (first and third party both) and cost of determining whether data held can be restored, recollected or recreated. • Business/network interruption coverage including System failure (Unintentional and unplanned outage of a computer system or damage, alteration, deletion, corruption or loss of Data) • Crisis management coverage • Forensic services • Professional fees for advice and representation of regulatory investigation; Professional Fees include costs incurred during 60 Hours of a qualifying breach of data security without prior consent of the Insurer- sub-limited to 10% of the limit of liability • Repair of company's Reputation • Repair of individual's Reputation • E-Communications Loss: sub-limited to INR 25,00,00,000 each and every accident and in aggregate • Media liability claims cover • Costs, Civil Fines and penalties wherever insurable by law • Defense of regulatory actions including failure to notify • Liability arising out of Outsourced Activities • Cover for non-compensatory damages, including but not limited to punitive, multiple, exemplary damages where insurable by law. • Cover for Civil fines & penalties wherever insurable by law • Cover for cleanup costs- Sub limited to 10% of the limit of Liability • Cover for Reward expenses- sub limited to 1% of the limit of liability with NIL retention • Goodwill coupon • Insured definition to include employees (full time and contractual), outsourced employees, consultants, Retainers, Trainees and subject matter experts solely under contract with and under the direct supervision of GSTN • No exclusion for Unauthorized Data Access/Intentional Act/Criminal Acts

	• Notice of claim/circumstance upon knowledge of the control group • Extended reporting period (90 days) • Amended discovery period: 90 days free and 365 days at 50% Annual Premium • Policy not to be cancelled except for non-payment of premium • Waiver of subrogation (wherever required by written contract) • No Unlawful or unauthorized data collected exclusion • Revamp costs Cover • Hardware and IT equipment Restoration cover • Pro Active response costs cover with Nil or retention not more than INR 5 lacs • Additional Insured Endorsement. • Psychological Support Expenses: 5% of Limitation of Liability in aggregate. • Court attendance Fee: Rs.30,000/- per employee and Rs.50,000/- per Director • Amended Insurer's Consent claue: That for any Claim where the total claim value, including Defence Costs and Damages combined, is less than 100% of any applicable Retention, the Insured may settle the Claim without the written consent of the Insurer • Multimedia claims without consent: To include defense cost incurred for Multimedia Liability without insurer's prior written consent • Cover for Credit Monitoring expenses incurred by the Insured • Cover for Proactive- forensics and investigation costs- cover to trigger in case of suspected events. • Amended computer system definition to include all GSTN systems, including but not limited to any allied or attached systems, cloud systems, GSTN's all projects/platforms (e.g. GST System, E-Way Bill, E-invoice System etc.), operations, systems and GST network.
Support Claims experience on GSTN	100% - 24x7 Nil Claims

Note: ***The bidder has to submit verbatim cyber insurance policy wordings (including proposed exclusion(s)) along with technical proposal.***

Also, please find attached the General and Cyber questionnaire as *Enclosure I to RFP* for ready reference.

2. Eligibility Criteria

2.1 Pre-Qualification Criteria

The bid must be complete in all respects and should cover the entire scope of work as stipulated in the document. Bidders / Insurers not meeting the Pre-Qualification Eligibility Criteria will not be considered for further evaluation.

The Eligibility Criteria as given below. Failure to provide the desired information and documents may lead to disqualification of the Bidder. Pre-Qualification will be scrutinized by the evaluation committee as constituted by GSTN to check all requisite and relevant documents and their authenticity.

Sr. No	Description	Documentary Proof to be attached
1	The Insurer must have an IRDA license for carrying on insurance business in India.	IRDA license copy
2	The Insurer must have a track record of minimum 3 years of operations in General insurance business in India as on 31st March 2025	IRDA Renewal Certificates for last three (03) Years i.e. 2022-23, 2023-24 & 2024-25
3	Insurer's Annual Average Gross written premium collection for the year's 2022-23, 2023-24 & 2024-25 should be at least ₹ 1000 Crs. (including Reinsurance)	Audited Annual Report OR CA Certified Financial Statement
4	The Insurer must have an existing relationship with at least 2 clients regarding the offer of Cyber Insurance. One client should be from Banking and/or Financial Sector.	The insurer should provide client's Name, Policy sum insured, and policy period. Wherever there is a problem in providing a name due to Non-disclosure agreements with the clients, the bidder can provide a certificate from an independent auditor or Company Secretary. The certificate should include the scope of work and policy sum insured and policy period.
5	The Insurer should not be blacklisted by Government/ Government Agency/ Bank / Institution in India.	Declaration as per ***Annexure II***

3. Evaluation of Proposal:

Method of Selection	The method of selection is Quality and Cost Base Selection **(QCBS).** The weights given to the Technical and Commercial Bids are: **Technical = 70%** and **Commercial = 30%**

- ***Technical Evaluation:-***

Each Technical bid will be assigned a technical score out of a maximum of **400 marks** (marks breakup described in **point 4 Section II**). Only the bidders who get a technical score of **65 percent or more** in each section and **70 percent or more** overall will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the bid.

The normalized technical score of the bidder shall be calculated as follows:

Normalized Technical Score of a bidder = {Technical Score of that bidder/Score of the bidder with the highest technical score} X 400 (adjusted to 2 decimals)

Final score calculation through QCBS (Quality and Cost Based Selection)

Example: Technical Score

Bidders	Technical score (B)	Normalized Technical Score	Normalized Technical Final Score
1	350	(350/390)*400	358.97
2	360	(360/390)*400	369.23
3	370	(370/390)*400	379.49
4	380	(380/390)*400	389.74
5	390	(390/390)*400	400.00

- ***Commercial Evaluation:-***

Technically qualified bidders as per technical evaluation process will participate in commercial bid opening process. The bidder will quote as per Price Format provided by GSTN **(Annexure–I)** and further evaluated as per following method:

Commercial Score

#	Citation	Citation Details	Documentary Evidence	Score
1.	Premium quoted	Normalised Score = (Lowest premium amongst the bidders /Premium by the bidder)*300	As per quote	
2.	Policy deductible	Normalised Score = (Lowest deductible amongst the bidders /Deductible by the bidder)*100	As per quote	
		Final Commercial Score		400

Example: Commercial Score

Bidders	Premium Quoted by bidders (in Lakhs)	Policy Deductible Quoted by bidders (in Lakhs)	Normalized Commercial Score for Premium Quoted	Normalized Commercial Final Score for Premium Quoted	Normalized Commercial Score for Deductible Quoted	Normalized Commercial Final Score for Deductible Quoted	Normalized Commercial Final Score
1	10	1	(10/10)*300	300.00	(1/1)*100	100.00	400.00
2	11	2	(10/11)*300	272.73	(1/2)*100	50.00	322.73
3	12	3	(10/12)*300	250.00	(1/3)*100	33.33	283.33
4	13	4	(10/13)*300	230.77	(1/4)*100	25.00	255.77
5	14	5	(10/14)*300	214.29	(1/5)*100	20.00	234.29

Final score calculation through QCBS

1. The final score will be calculated through Quality and Cost based selection method with the following weightage:

Technical: 70% Commercial: 30%

Final Score = (0.70*Normalized Technical Final Score) + (0.30* Normalized Commercial Final Score)

Bidders	Normalized Technical Final Score	Normalized Commercial Final Score	Final Score (70:30)
1	**358.97*.7**	**400*.3**	**371.28**
2	369.23*.7	322.73*.3	355.28
3	379.49*.7	283.33*.3	350.64
4	389.74*.7	255.77*.3	349.55
5	400*.7	234.29*.3	350.29

The bids with Highest Final Score will be selected.

4. Quality and Cost Based Selection (Evaluation):

4.1 Technical Evaluation Framework:

The bidder's technical solution proposed in the technical evaluation bid document will be evaluated as per the evaluation criteria mentioned in the table below:

#	Evaluation Criteria	Total Marks	Minimum Qualifying normalized Marks (Cut-off)
1	Gross underwritten premium for Standalone Cyber Liability policies for IT / ITES industries in last financial year ending 31st March, 2025	100	>=65 (65%)
2	Highest Sum Insured contributed for Standalone Cyber Liability policy for IT/ ITES industries for last financial year ending 31st March, 2025	100	>=65 (65%)
3	Solvency Ratio	100	>=65 (65%)

4	Maximum own net and treaty capacity Cyber insurance policies for IT/ ITES sector in last financial year ending 31st March, 2025	50	>=32.5 (65%)
5	Time deductible(i.e. waiting period for network interruption)	50	>=32.5 (65%)
Total		***400**	**>=280 (70%)**

***Exclusion(s) incorporated in cyber insurance policy may result in negative marking subject to a maximum forty (40) marks in final technical score depending upon the impact of exclusion(s) on the coverage. GSTN decision in this regard will be final and binding on the bidder.**

GSTN (or a nominated party) reserves the right to check/validate the authenticity of the information provided in the pre-qualification and Technical evaluation criteria and requisite support must be provided by the bidder.

The following sections explain how the Insurers will be evaluated on each of the evaluation criteria.

4.2 Technical Score

#	Citation	Citation Details	Documentary Evidence	Score
1.	Gross underwritten premium for Standalone Cyber Liability policies for IT / ITES industries in last financial year ending 31st March, 2025 ***(Amount in Cr.)***	Insurer must have underwritten Cyber insurance policies for IT/ ITES sector. The premium to be taken into account shall be own share in a policy having multiple insurers if any. The marks shall be allotted as below: Gross Premium >=3 Cr. & < 4 Cr. = 65 marks >=4 Cr. & < 5 Cr. = 70 marks >=5 Cr. & < 8 Cr. = 80 marks >=8 Cr. & < 10 Cr. = 90 marks >=10 Cr. & = 100 marks **(Max. Marks = 100)**	Certified by Independent/ Statutory Auditor	
2.	Highest Sum Insured contributed for Standalone Cyber Insurance for IT/ ITES industries for last financial year ending 31st March, 2025 ***(Amount in Cr.)***	Insurer's highest sum insured placed for Cyber insurance policies The marks shall be allotted as below: Highest Sum insurance >=25 Cr. & <30 Cr. = 65 marks >=30 Cr. & < 35 Cr. = 70 marks >=35 Cr. & < 40 Cr. = 80 marks >=40 Cr. & < 50 Cr. = 90 marks >=50 Cr. = 100 marks **(Max. Marks = 100)**	Certified by Independent/ Statutory Auditor	

3.	Solvency Ratio	Please indicate the Solvency ratio as per your Public Disclosure for the period ending March, 2025 The marks shall be allotted as below: Solvency Ratio >= 1.5 & < 1.65 = 65 marks >=1.65 & <1.75 = 75 marks >=1.75 & <2.00 = 85 marks >=2.00 =100 marks **(Max. Marks = 100)**	Copy of Public Disclosure report OR Certified by Independent/ Statutory Auditor	
4.	Maximum own net and treaty capacity you have for Cyber insurance policies for IT/ ITES sector in last financial year ending 31st March, 2025 ***(Amount in Cr. only)***	The marks shall be allotted as below: Net and Treaty Capacity >=20 Cr. & < 25 Cr. = 32.5 marks >=25 Cr. & < 30 Cr. = 35 marks >=30 Cr. & < 40 Cr. = 40 marks >=40 Cr. & < 50 Cr. = 45 marks >=50 Cr. = 50 marks **(Max. Marks = 50)**	Certified by Independent/ Statutory Auditor	
5.	Time deductible (i.e. waiting period for network interruption)	Please mention the Time deductible in the technical proposal The marks shall be allotted as below: Time deductible 12 Hours = 35 marks 08 Hours = 40 marks ≤04 Hours = 50 marks **(Max. Marks = 50)**	Bidder has to mention the Time deductible in their Technical Proposal	
Final Technical Score				*400
The minimum aggregate qualifying score				280

***Exclusion(s) incorporated in cyber insurance policy may result in negative marking subject to a maximum forty (40) marks in final technical score depending upon the impact of exclusion(s) on the coverage. GSTN decision in this regard will be final and binding on the bidder.**

Note:

It is clarified that maximum marks 100 for solvency ratio ranging from 1.5 to 2.00 (S. No. 3 of clause no. 4.1 Technical Evaluation Framework and 4.2 Technical Score) will be exempted for Public Sector Insurance Companies in line with directive of Ministry of Finance order no. F.No - EG- 14017/64/2020-InsII dated 02.07.2022. Hence, marks obtained by Public Sector Insurance Companies on basis of remaining 300 marks will be extrapolated / rationalized to 400 marks on basis of formula given below:-

Total Marks obtained by Public sector Company (from a total score of 400 marks)= {Total Marks Obtained by Public sector Company (from a total score of 300 marks)/300}*400

SECTION – III: GENERAL INSTRUCTIONS TO BIDDER

1. SUBMISSION OF PROPOSALS:

a) All bidders are required to submit their bids as per Quotation Sheet attached as **Annexure I** on Insurance Company's Letter Head only. Bids submitted in any other format shall not be accepted and treated as non-responsive. The bidder shall quote for all the items listed in the Quotation sheet **(Annexure I)** failing which the bid shall be considered nonresponsive and shall not be considered for evaluation.

b) All the bidders are requested to quote as per IRDAI guidelines. Any quotation found to be in breach of IRDAI guidelines shall be rejected. Bid should be mapped with Indian Regulation only.

c) Empaneled Insurance Brokers are requested to submit the Compliance declaration as per the format enclosed at **Annexure-VI** and No deviation certificate as per format enclosed at **Annexure -IV** alongwith their bids on Insurance Companies letter head**.** The selected Insurer (Insurance Company) have to sign the Non-Discloser Agreement (NDA) as per **Annexure-III**.

d) The Empaneled Insurance Brokers are expected to scrutinize all instructions, inclusions/exclusions, terms and conditions of the bidding document (insurance policy being offered by Insurance companies). Bid with any deviation is liable to be rejected.

2. BID PRICE:

a) The prices should be quoted in Indian Rupees with delivery of item at GSTN, failing which the bid would be rejected. The price shall be written both in figures & words in the prescribed offer form.

b) If, in the price structure quoted by a bidder, there is discrepancy between the unit price and the total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price corrected accordingly.

c) If there is an error in a total price, which has been worked out through addition and/or subtraction of subtotals, the subtotals shall prevail and the total corrected; and

d) If there is a discrepancy between amount in words and figures, the amount in words will prevail.

e) If, one of the conditions mentioned above a, b, c & d occurs, the same will be conveyed to the L1 bidder by e-mail. If the L1 bidder does not agree to the observation of GSTN so conveyed, the bid will be ignored.

f) Incomplete and/or conditional bids shall be liable to rejection.

3. VENUE & DEADLINE FOR SUBMISSION OF PROPOSALS:

a) Proposals, in its complete form in all respects as specified in the RFP, must be submitted to Goods and Services Tax Network (GSTN) as specified in the Key

details Table.

b) Last Date & Time of submission: As given in the Key details Table

c) Goods and Services Tax Network (GSTN) may, in exceptional circumstances and at its discretion, extend the deadline for submission of proposals by issuing an addendum, in which case all rights and obligations of Goods and Services Tax Network (GSTN) and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

4. LATE BIDS:

Bids received after the due date and time as specified in the RFP Notification Table (including the extended period if any) for any reason whatsoever, shall not be entertained by Goods and Services Tax Network.

5. VALIDITY OF QUOTATION:

Proposal shall remain valid for a period of **60 days** from the date of bid opening.

6. LANGUAGE:

The bid and all related correspondence and documents in relation to the bidding process shall be in English language.

Supporting documents and printed literature furnished by the bidder with the bid may be in any other language provided that they are accompanied by translations of all the pertinent passages in the English language, duly authenticated and certified by the bidder.

Supporting materials, which are not translated into English, may not be considered. For the purpose of interpretation and evaluation of the bid, the English language translation shall prevail.

7. ACCEPTANCE OF TERMS & CONDITIONS:

Empaneled Insurance Brokers are requested to get a sealed and signed copy of this RFP document from Insurance Companies and submit it along with quotation as acceptance of all terms & conditions. In case signed & stamped copy of this RFP is not submitted, it will be assumed that the Insurance Company will, by responding to GSTN's RFP/Tender document, be deemed to have accepted all the terms as stated in this RFP/Tender document.

8. GOODS AND SERVICES TAX NETWORK'S RIGHT TO TERMINATE THE PROCESS:

a) Goods and Services Tax Network (GSTN) reserves the right to accept or reject any proposal, and to annul the bidding process and reject all proposals at any time prior to award of agreement, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for actions taken by Goods and Services Tax Network.

b) GSTN is accepting the bids on a no cost no commitment basis.

c) Goods and Services Tax Network (GSTN) makes no commitments, express or implied, that this process will result in a business transaction with anyone.

9. ACCEPTANCE OF PART / WHOLE BID / MODIFICATION – RIGHTS THERE OF:

Goods and Services Tax Network (GSTN) reserves the right to accept or reject wholly or partly bid offer, or modify the requirements mentioned in this RFP including addition/ deletion of any of the item or part thereof after pre-bid, without assigning any reason whatsoever. No correspondence in this regard shall be entertained.

10. COSTS TO BE BORNE BY THE BIDDER:

All costs and expenses (whether in terms of time or money) incurred by the intended bidder in any way associated with the development, preparation and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by GSTN, will be borne entirely and exclusively by the bidder itself.

11. ALTERATION AND WITHDRAWAL OF RFP:

a) The bidder, after submitting its RFP, is permitted to alter / modify its RFP so long as such alterations / modifications are received duly signed, sealed and marked like the original RFP, within the deadline for submission of RFPs. Alterations / modifications to RFPs received after the prescribed deadline will not be considered.
b) No RFP should be withdrawn after the deadline for submission of RFP and before expiry of the RFP validity period.

12. JURISDICTION:

This Agreement shall be subject to exclusive jurisdiction of courts at Delhi only.

SECTION – IV: GENERAL CONDITIONS OF THE CONTRACT (GCC)

1. DELIVERY PERIOD:

The risk acceptance cover letter shall be delivered within two working days and formal Insurance policy document confirming cover shall be delivered within 30 days from the date of the Payment.

2. PAYMENT TERMS:

100% payment would be released through RTGS/NEFT on receipt of the following details:

1. Proforma invoice duly signed by the authorized signatory.
2. PAN Card, Bank Account Details, Bank address & RTGS details of the Agency are to be forwarded along with the Invoice.

3. COMMERCIAL BID EVALUATION CONSIDERATIONS:

Commercial bid evaluation shall be considered as below in case of any kind of discrepancy:

Commercial Bid Evaluation

a. Only fixed price financial bids indicating total price, as specified in **Annexure-I**, Financial Proposal 'Commercial Quotation' for all the services specified in this RFP document will be considered.

b. The bidder shall quote the price as per specified format for the entire policy period on a single responsibility basis. The price shall be quoted entirely in Indian Rupees and taxes will be paid on actual basis. The price shall be written both in figures & words in the prescribed offer form.

c. For all the quoted prices and the numbers used during the process defined above, only two digits after decimal will be considered for calculation purposes and the same will be subject to standard rounding rules.

d. The prices, once offered, must remain fixed and must not be subject to escalation for any reason whatsoever within the period of policy. A bid submitted with an adjustable price quotation or incomplete or conditional bid may be rejected as non-responsive.

e. Any change in tax upward/downward as a result of any statutory variation in tax taking place within contract terms shall be allowed to the extent of actual quantum of Tax paid by the Insurance Company. In case of downward revision in tax, the actual quantum of reduction of tax shall be reimbursed to GSTN by the Insurance Company.

f. Errors & Rectification: Arithmetical errors will be rectified on the following basis:

   i. If, in the price structure quoted by a bidder, there is discrepancy between the unit price and the total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price corrected accordingly.

   ii. If there is an error in a total price, which has been worked out

through addition and/or subtraction of subtotals, the subtotals shall prevail and the total corrected; and

iii. If there is a discrepancy between the amount expressed in words and figures, the amount in words shall prevail,

iv. If, as per the judgment of GSTN, there is any such arithmetical discrepancy in a bid, the same will be suitably conveyed to the bidder by post or e-mail. If the bidder does not agree to the observation of GSTN, the bid is liable to be ignored.

ANNEXURE-I: PRICE FORMAT

Table A

Sr. No.	Description	Premium Amount (INR) (A)	Tax Rate %	Tax Amount (INR) (B)	Total Premium Amount (INR) inclusive of Taxes (C = A+B)
1.	Cyber Risk Insurance				
	Total Bid Price inclusive of Taxes:				
Amount in words: Rupees.....					

Table B

Sr. No.	Description	Amount (INR)
1.	Policy deductible	
Amount in words: Rupees		

Note: i. Price quoted should be inclusive of all taxes and all other additional charges
ii. Taxes will be paid on actual basis.

Signature with Stamp of Authorized Person

Date: Full Name:

Place: Company's Seal:

ANNEXURE-II: PROFORMA FOR NOT BEING BLACKLISTED

(To be submitted on the Letterhead of the Insurer)

(Place)

(Date)

To
VP (P&C)
Goods and Services Tax Network
4th Floor, Worldmark-1, East Wing, Aerocity,
New Delhi-110037

Dear Sir,

We confirm that our company is not blacklisted in any manner whatsoever by Goods and Services Tax Network, any State Government, Central Government or any other Public sector undertaking or a Corporation or any other Autonomous organisation of Central or State Government as on Bid submission date.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

[on behalf of *Insurer Name]*
Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Firm:
Address:
Seal/Stamp of Insurer:

ANNEXURE-III: NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement ("Agreement") is entered into on this the ____ day of _____, 2025 between:

Goods and Services Tax Network, a company registered under section 8 (under new companies Act, not for profit companies are governed under section 8), having its registered office at 4th Floor, Worldmark – 1, East Wing, Aerocity, New Delhi – 110037, India (Hereinafter referred to as "GSTN", which term shall, unless repugnant to the context or meaning thereof, mean and include its successors and permitted assign) of the FIRST PART;

AND

M/s_____, ("_____"), a company incorporated under the _____, having its Registered office at _____, (which expression shall, unless repugnant to the context thereof, mean and include its successors and assigns) of the SECOND PART;

(Hereinafter individually referred to as "Party" and collectively referred to as "Parties".)

RECITALS:

A. The Party of the FIRST PART is desirous to hire the Party of the SECOND PART for certain services ("Services"). The Party of the SECOND PART has agreed to provide the said Services by entering into a separate agreement ("Service Agreement") for that purpose. During the time of negotiation and after the execution and term of the aforesaid Service Agreement, while the Party of the SECOND PART will be providing the aforesaid Services to the Party of the FIRST PART, the Parties may disclose certain confidential information with each other which could be sensitive, critical and peculiar to their respective businesses.

B. This Agreement looks at determining and regulating the disclosures made by the Parties hereto of confidential information in connection with the negotiations and execution and performance of the Service Agreement between the Parties (hereinafter "the Purpose").

NOW IT IS HEREBY AGREED AS FOLLOWS:

1. The Parties agree to execute this Confidentiality Agreement and be bound by the terms and conditions hereof as a precondition to the proposed negotiations/discussions and agreement between the Parties in relation to the Purpose.

2. "Confidential Information" shall mean all information, know-how, ideas, designs, documents, concepts, technology, manufacturing processes, industrial, marketing, commercial knowledge, and other materials of a confidential nature and includes but is not limited to, information of a commercial, technical or financial nature which contains amongst other matters, trade secrets, know-how, patent, IPRs and ancillary information and other proprietary or confidential information, regardless of form, format, media including without limitation written or oral, and also includes those communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site or place including without limitation:

   i) research, development or technical information, confidential and proprietary information on products, intellectual property rights;
   ii) business plans, operations or systems, financial and trading positions;
   iii) details of customers, suppliers, debtors or creditors;

iv) information relating to the officers, directors or employees of the Disclosing Party and background verification in relation thereto;
v) formulae, IPRs, patterns, compilations, programmes, devices, methods, techniques, or processes, that derive independent economic value, actual or potential, from not being generally known to the public.

3. Except as otherwise provided in this Agreement, the Party receiving Confidential Information ("Receiving Party") shall keep confidential all information of the Party disclosing Confidential Information ("Disclosing Party") which:

(a) is disclosed, communicated or delivered to the Receiving Party in furtherance to the Purpose for which the Parties are entering into negotiations/discussions;

(b) comes to the Receiving Party's knowledge or into the Receiving Party's possession in connection with negotiations/discussions towards the Purpose.

Notwithstanding whether such Confidential Information is received before or after the date of this Agreement.

4. Except as otherwise provided in this Agreement, the Receiving Party shall not disclose to any other person the status, terms, conditions or other facts concerning the negotiations/discussions as contemplated between the Parties in terms hereof.

5. The Receiving Party shall not use or copy the Confidential Information of the Disclosing Party except in connection with the Purpose and as both Parties may agree in writing from time to time.

6. In the event of the Receiving Party visiting any of the facilities of the Disclosing Party, the Receiving Party undertakes that any further Confidential Information which may come to its knowledge as a result of any such visit shall be kept strictly confidential and that any such Confidential Information will not be divulged to any third party and will not be made use of in any way, (whether for its benefit or that of any third party) except in connection with the Receiving Party's negotiations with the Disclosing Party in terms hereof.

7. Except as otherwise provided in this Agreement, the Receiving Party shall not disclose or communicate, cause to be disclosed or communicated or otherwise make available Confidential Information to any third party other than:

(a) the Receiving Party's directors, officers, employees, or representatives to whom disclosure is necessary for the purpose of negotiations/discussions;
(b) the Receiving Party's professional adviser only to the extent necessary for that adviser to advice or protect the rights of the Receiving Party under this Agreement;
(c) the Receiving Party's appointed financial adviser or appointed banker only to extent necessary for the financial adviser or appointed banker to provide financial advice and/or financial services to the Receiving Party.
(each an "Authorised Person", and collectively, the "Authorised Persons").

8. The Receiving Party hereby agrees to bind such Authorised Person(s) and Re-insurer(s) with similar obligations of confidentiality. In any event, the Receiving Party shall remain liable for any disclosure by the Authorised Person(s) and Re-insurer(s) to any other person.

9. The Receiving Party's obligations hereunder shall not apply to Confidential Information if the same is:
   (a) in or enters the public domain, other than by breach by the Receiving Party or any of its Authorised Person(s) or
   (b) known to the Receiving Party on a non-confidential basis prior to disclosure under this Agreement, at the time of first receipt, or thereafter becomes known to the Receiving Party or any of its Authorised Person(s) without similar restrictions from a source other than the Disclosing Party, as evidenced by written records, or
   (c) is or has been developed independently by the Receiving Party without reference to or reliance on the Disclosing Party's Confidential Information.

10. Except as otherwise provided in this Agreement, a Receiving Party may not disclose the Confidential Information of the Disclosing Party except if the disclosure is made pursuant to a directive or order of a Government entity or statutory authority or any Judicial or governmental agency provided however that the Receiving Party shall promptly notify the Disclosing Party so as to enable the Disclosing Party to seek a protective order or other appropriate remedy;

11. The Receiving Party shall exercise no lesser security or degree of care than that Party applies to its own Confidential Information of an equivalent nature, but in any event, not less than the degree of care which a reasonable person with knowledge of the confidential nature of the information would exercise.

12. The Receiving Party acknowledges that any breach of this Agreement by the Receiving Party may cause the Disclosing Party irreparable damage for which monetary damages may not be an adequate remedy. Accordingly, in addition to other remedies that may be available, the Disclosing Party may seek injunctive relief against such a breach or threatened breach.

13. All written Confidential Information or any part thereof (including, without limitation, information incorporated in computer software or held in electronic storage media) together with any analyses, compilations, studies, reports or other documents or materials prepared by the Receiving Party or on its behalf which reflect or are prepared from any of the Confidential Information provided by the Disclosing Party shall be returned to the Disclosing Party or destroyed by the Receiving Party, when requested by the Disclosing Party at any time, or when the Receiving Party's need for such information has ended or when this Agreement expires or is terminated, whichever is earlier. In the event of destruction, the Receiving Party shall certify in writing to the Disclosing Party within thirty (30) days, that such destruction has been accomplished. The Receiving Party shall make no further use of such Confidential Information nor retain such Confidential Information in any form whatsoever. Provided, however, Receiving Party may retain copy of such Confidential Information for the purposes of and for so long as required by any law, court or regulatory agency or authority or its internal compliance procedures and for archival, back-up purposes only, the confidentiality obligation shall continue until such information is retained.

14. This Agreement shall be effective and binding from the date of execution hereof and will continue during the term of the Service Agreement, until and unless terminated in accordance with clause 15 herein.

15. This Agreement shall terminate upon the occurrence of the earlier of the following events:
   (a) the termination of the Service Agreement before the completion of the term thereof;
   (b) by written agreement between the Parties;

(c) when either Party notifies the other in writing electing to discontinue the negotiations and discussions in respect of the Purpose;

16. Notwithstanding the expiration/termination of this Agreement, the obligation to maintain confidentiality of the Confidential Information provided hereof and the undertakings and obligations in this Agreement shall continue for a period of five (5) years from the date of expiration or termination of the Agreement, as the case may be.

17. Nothing contained in this Agreement shall be deemed to grant to the Receiving Party either directly or by implication, any right, by license or otherwise, under any patent(s), patent applications, copyrights or other intellectual property rights with respect to any Confidential Information of the Disclosing Party nor shall this Agreement grant Receiving Party any rights whatsoever in or to the Disclosing Party's Confidential Information, except the limited right to use and review the Confidential Information as necessary to explore and carry out the proposed Purpose between the Parties.

18. This Agreement is not intended to constitute, create, give effect to, or otherwise recognize a joint venture, partnership or formal business entity of any kind and the rights and obligations of the Parties shall be limited to those expressed set forth herein. Any exchange of Confidential Information under this Agreement shall not be deemed as constituting any offer, acceptance, or promise of any further contract or amendment to any contract which may exist between the Parties. Nothing herein shall be construed as providing for the sharing of profits or losses arising out of the efforts of either or both parties. Each Party shall act as an independent contractor and not as an agent of the other Party for any purpose whatsoever and no Party shall have any authority to bind the other Party.

19. This Agreement contains the entire understanding between the Parties with respect to the safeguarding of said Confidential Information and supersedes all prior communications and understandings with respect thereto. No waiver, alteration, modification, or amendment shall be binding or effective for any purpose whatsoever unless and until reduced to writing and executed by authorized representatives of the Parties.

20. The rights, powers and remedies provided in this Agreement are cumulative and do not exclude the rights or remedies provided by law and equity independently of this Agreement.

21. This Agreement shall be governed and construed in all respects in accordance with the laws of India.

IN WITNESS WHEREOF BOTH PARTIES HAVE PUT THEIR SIGNATURES ON THE DAY HEREIN ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED	SIGNED, SEALED AND DELIVERED
For and on behalf of the GSTN by: (Signature) (Name) (Designation)	For and on behalf of the (name of company) by: (Signature) (Name) (Designation)

IN WITNESS WHEREOF the Parties have by duly authorized Representatives set their respective hands and seal on the date first above Written in the presence of:

For GSTN	For _____(name of company)
Witness 1:	Witness 1:
Witness 2:	Witness 2:

ANNEXURE-IV: NO DEVIATION CERTIFICATE

(To be submitted on Insurance Company's Letter Head)

This is to certify that our submitted proposal is exactly in line with the requirements outlined in your RFP No. GSTN/P&C/CISO/CI/08-2025/P-12 dated ..... (including corrigendum, if any).

This is to expressly certify that there are no deviations, whether direct or indirect, from the scope of insurance coverage required for the Cyber policy.

Our Proposal (and/or the policy to be issued, in case we are declared the H1 bidder) fully adheres with all the Details of Requirement specified in this RFP, including any corrigendum issued thereafter.

This declaration is made in full conformity with the tender requirements, and any deviation, if found, may render our bid liable for rejection. Furthermore, in the event that a claim arises at any stage prior to the bid rejection date and time and such a claim falls within the scope and coverage defined in the RFP and its corrigendum, it shall be our responsibility, as the insurance provider, to process and settle the claim by insurance company in accordance with the terms and conditions of RFP and its corrigendum during the validity of the policy period.

(Authorised Signatory)

Signature:
Name:
Designation:
Address:

Seal:
Date:

ANNEXURE V – REQUEST FOR CLARIFICATION FORMAT

(To be submitted in excel format only)

1. Company Name:

2. Name and Designation of person submitting the request:

3. Full formal address of the bidder including phone, fax and email points of contact:

S. No.	RFP / Tender Document Reference(s) (section number/ page)	Content of RFP / Tender requiring Clarification	Points on which clarification required
1			
2			

ANNEXURE VI – COMPLIANCE DECLARATION

1. I/We, ... Proprietor / Partner / Director / Authorized Signatory of M/s. Name of Insurance Company have carefully read and understood all the terms and conditions of the RFP and hereby express that all the required coverage/features, terms and conditions stated in the RFP are acceptable to us.

2. I/We confirm that the decision of GSTN with regard to this RFP will be binding on us.

3. The information / documents contained in our bid are true and authentic to the best of my/our knowledge and belief. I/We, am/are well aware of the fact that furnishing of any false information / fabricated document would lead to rejection of my/our bid at any stage besides liabilities towards prosecution under appropriate law.

Date:

Signature of Authorized Signatory:

Name & Designation:

Seal of the Company

RFP Ref. No.: GSTN/P&C/CISO/CI/08-2025/P-12 Date: 04/09/2025

Enclosure I to RFP

General and Cyber Questionnaire

GOODS AND SERVICES TAX NETWORK (GSTN)
4th Floor, East Wing, World Mark-1, Aerocity,
New Delhi – 110037
Tel: 011-49111200, Fax: 011-49111210
ebsite: www.gstn.org.in

S.No.	Questions	GSTN's Response	Additional Remarks
	General		
1	Name of Applicant(including subsidiaries)	Goods and Services Tax Network (GSTN), a company registered under Section 8 of the New Companies Act	No Subsidiaries
2	Principal Address of Applicant(including subsidiaries)	East Wing, 4th Floor, World Mark - 1, Aerocity, New Delhi-110037	No Subsidiaries
3	Website	www.gstn.org.in www.gst.gov.in www.ewaybillgst.gov.in www.e-invoice.gst.gov.in	
4	Business Description	To provide IT infrastructure and services to the Central and State Governments, tax payers and other stakeholders for implementation of the Goods and Services Tax (GST)	
5	Gross Revenue (Local Currency)	**Prior Year**	**Current Year**
		NA	NA
6	Geographical Split of the organization's Total Gross Revenue (%)	**Prior Year**	**Current Year**
	European Union	NA	NA
	Canada	NA	NA
	United States	NA	NA
	India	NA	NA
	Rest of World	NA	NA
7	Details of operating locations and data center locations	DC1/NDC1 - Delhi DC2/NDC2- Bangalore	
8	List of subsidiaries to be covered? - Kindly confirm if whether all the subsidiaries of the Insured share a common internal network? - or, are the networks of subsidiaries along with Insured connected	NA	
9	Please let us know if the IT security principles/policies/infrastructure and the team managing the function is centralized or decentralized. This needs to be in context all the entities (subsidiaries and manufacturing locations and offices including global entities if any) proposed to be covered under the policy	Centralized team headed by CISO	
10	Number of employees in the financial year (with break-up (India/ROW/USA&Canada)	India Only, 120 (Approx.)	
11	Number of online customers and revenue Generated through online Sale with region-wise break-up (India/ROW/USA&Canada)	NA	
12	Are there planned Mergers or Acquisitions for the next 12 months?	Yes/No - NO	
13	Have any mergers or acquisitions taken place in the last 5 Years?	Yes/No/Not Applicable - NO	
	If yes, please share brief detail how security policies, processes have been integrated with main group	NA	
14	Is organization compliant with any of the following regulatory or compliance frameworks? a. ISO 27001:2013 Information security management system b.COBIT 5 c. HIPAA d. GDPR Also, mention date of compliance.	Certified with following a) ISO 27001:2022, ISO 20000, ISO 22301 Information security management system b.COBIT 2019	HIPAA & GDPR not applicable
15	Do third parties rely on the availability of the organization's technology platforms (such as website(s), data processing services, hosting services, internet transactions, etc.) to transact business?	Yes/No/Not Applicable - No	Taxpayers, Tax officers, GSP's, Helpdesk etc are performing GST filing related activities.
16	If the answer to the above question is yes, please indicate whether the third-parties conduct business or consumer activity and how much of their revenue is dependent on the use of the organization's technology platforms. (B-B/ B-C)		

S.No.	Questions	GSTN's Response	Additional Remarks
	Data Protection & Privacy		
1	Kindly confirm if you have a documented: a. Data Protection & Privacy Policy b. Information Security Policy c. Guidelines on the retention, storage, handling and disposal of records and information Please also mention who has reviewed and approved the policy documents.	a. Yes/No - **YES** b.Yes/No - **YES** c. Yes/No - **YES**	GSTN/GST system is Certified against ISMS,ITSMS and BCMS. The certificates are valid till FY - 2026. All the policies/process etc are aligned with the same.
	If "No", please provide details regarding respective measures adopted by the organization to ensure information security/data protection & Privacy/ retention/storage handling and disposal of records and information		
2	In reference to point 1, are these policy/guidelines documents shared with all employees, third parties(wherever required) including any updates?	Yes /No - Yes	
	If "No" please explain why not:		
3	Please mention the type of data records held(collect, store, process and/or transmit)by the organization: (Mention the range of data as well for e.g.. 1 million records of PHI data etc.)		
	a.Personally Identifiable Information (PII)	Yes /No & mention range - **YES**	
	b. Payment Card Information (PCI)	Yes /No & mention range - **NO**	
	c. Protectable Health Information (PHI)	Yes /No & mention range - **NO**	
	d. Intellectual property (IP)	Yes /No & mention range - NO	
	e. Other (Please specify)	Yes /No & mention range	
4	Does the organization outsource any data collection and/or data processing activity?	Yes /No/Not Applicable - NO	
	If Yes", please provide details of the data collection or data processing functions which are outsourced		
5	Does the organization require the entities providing data collection or data processing functions (Outsourcers) to maintain their own data protection liability insurance?	Yes /No/Not Applicable - NA	
6	Does the organization's data protection and privacy policy comply with the data protection and privacy legislation applicable to all jurisdiction and Industry standards/requirements, in which the organization operates?	Yes /No/Not Applicable - Yes	Limited to Indian compliances.
	If "No" please provide an explanation regarding non-compliance in all applicable jurisdictions:		
7	Has the organization appointed a designated personnel for following roles: a. Chief Compliance Officer b. Data Protection Officer and/or In-house Counsel responsible for data protection related matters c. Chief Information Security Officer (CISO)	a. YES b. YES c. YES	
	If "No" who is responsible within the organization for data protection and information security related matters?		
	Network Security		
8	Does the organization has a defined process to identify, detect and remediate network security issues	Yes/No - Yes	GSTN/GST system is Certified against ISMS,ITSMS and BCMS. The certificates are valid till FY - 2026. All the policies/process etc are aligned with the same.
9	Does the organization has a dedicated Security Operations Center (SOC) operating 24*7. If yes, then please mention whether: a. there is a staff dedicated to monitoring security operations ("Security Operations Center") B. it is operating 24/7 by a 3rd party (such as a Managed Security Services Provider) c. SOC has 24/7 monitoring of security operations by internal team	a.Yes/No - Yes b.Yes/No - Yes c. Yes/No - Yes	Dedicated SOCC operating 24x7x365 is implemented by MSP.
10	Does the organization has a dedicated Network Operations Center (SOC) operating 24*7 managed by in-house team or by 3rd party ?	Yes/No - Yes	Dedicated NOC operating 24x7x365 is implemented by MSP.
11	Has the organization implemented: a.host-based firewall solutions b. Advanced Persistent Threat (APT) c. User Entity Behavior Analysis (UEBA) d.Next-Generation Firewall (NGFW) or Unified Threat Management (UTM) solution capable of in-line Deep Packet Inspection (DPI)	a.Yes/No YES b.Yes/No YES c. Yes/No YES d.Yes/No YES	
12	Does the organization has implemented network segmentation to restrict lateral movement. If yes, then specify whether a. network is segmented by geography b. network is segmented by business function c. host firewall rules are implemented to prevent the use of RDP to log into workstation d. all service accounts deny interactive logons	a.Yes/No YES b.Yes/No YES c. Yes/No YES d.Yes/No YES	
13	Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?	Yes/No YES	
14	Does the organization have a Network Access Control (NAC) solution in place to allow the organizations to restrict access to resources on their network?	Yes/No YES	
15	Has the organization implemented strong authentication protocols for wireless networks to prevent wireless security attacks?	Yes/No Yes	
16	Is Email Sender Policy Framework (SPF) strictly enforced?	Yes/No YES	
17	Are email gateway configured to look for potentially malicious links, programs and block executables? Please also mention if organization has process to report suspicious emails to Internal security team	Yes/No YES	
18	Does the organization 'tags' or otherwise marks emails from outside the organization	Yes/No YES	
19	Please mention if email Protocol like Domain based Authentication reporting and conformance (DMARC) is in place	Yes/No YES	

S.No.	Questions	GSTN's Response	Additional Remarks
20	Please mention whether: a. organization uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables b.e-mail filtering solution blocks suspicious messages based on their content or attributes of the sender c.e-mail filtering solution has the capability to run suspicious attachments in a sandbox.	a. Yes/No YES b.Yes/No YES c. Yes/No NA	The E-mail in GST System is only outbound, Inbound E-Mail use case is not relavent.
21	Has the organization implemented a Network-based Intrusion Detection and Prevention (NIDS/NIPS) solution to detect and prevent any malicious activity by monitoring the network traffic?	Yes/No YES	
22	Does the organization monitor network traffic for anomalous, potentially suspicious data transfers and also for, performance and storage capacity issues	YES	
23	Has the organization implemented following: a. an Enterprise Threat Protection (ETP) DNS proxy to detect and prevent any malicious activity ingress to the organization b. Deception Tools & Honeypots solution to divert and detect attackers with no risk to real data, operations, or users	a.Yes/No YES b. Yes/No YES	
24	Please specify if the organization conducts: a. penetration testing and Vulnerability Assessment periodically in every financial year (including each time new systems are introduced and or major changes takes place). b. periodic IT Audits Does the organization ensure that all the critical observations are remediated as per defined timeline.	YES YES	
25	Does your web-server encrypt confidential data (e.g. HTTPS)?	YES	
26	Has the organization implemented a a.Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode b.host-based intrusion detection and prevention solution (HIDS/HIPS) on end-user devices and servers c. Load Balancer to maintain the availability of critical resources d.Anti-Distributed Denial-of-Service (DDoS) solutions to prevent DDoS attacks e. Patch management process and solution Please mention if any external service is used to monitor organization's attack surface (external/internet facing systems).	a.Yes/No YES b.Yes/No YES c. Yes/No YES d.Yes/No YES e.Yes/No YES	
27	Does the organization follow target time to deploy 'critical' – the highest priority – patches. If yes, a. within 24 hours b. 24-72 hours c. 3-7 days d. > 7 days Please also mention year to date compliance with its own standards for deploying critical patches such as 95% etc.	Yes/No, numeric value for target time and compliance percentage YES - Within 24 Hrs	
28	Please mention if: a. organization uses web filtering solution to stop employees from visiting malicious web pages b. web filtering solution blocks known malicious or suspicious download including executables c. web filtering capabilities are effective on all corporate assets, even if the corporate asset is not on a corporate network (e.g. assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet). d. organization block uncategorized and newly registered domains using web proxies or DNS filters.	a.Yes/No YES b.Yes/No YES c. Yes/No YES d.Yes/No YES	
29	Has organization implemented anti-virus protection on all end point devices, e-mail systems and servers	Yes/No YES	
	If "yes" does it use advanced heuristic- and behavioral-based detection mechanisms to protect against new malware	YES	
	Please mention if organization has an internal group which monitors the output of endpoint security tools and investigates any anomalies.	Yes/No - YES	
30	Please mention if organization has implemented EDR (Endpoint detection & response) solution with behavioral detection capabilities	Yes/No - YES	
31	Has the organization implemented a Data Loss Prevention (DLP) tool in monitor mode for making sure that end users do not send sensitive or critical information outside the corporate network?	Yes/No - NA	DLP usecase is not relavent in GST System.
32	Has the organization implemented a a.Mobile Device Management (MDM) solution to monitor, manage, and secure employee's mobile devices (*question applicable when employees can access official email or organizational applications from their mobile phones*) b. Database Activity Monitoring (DAM) Solution to detect and prevent malicious behavior in the database	a. Yes/No NA b. Yes/No YES	
	Backup & Recovery		
33	Kindly confirm if you have following: a. documented backup and recovery process b. offline backups are taken (can be stored on site) c. backup copies are stored at offline site d. Please specify the backup frequency of business critical data, systems e.backups are carried out as per defined frequency for business critical data, does real time data replication also takes place ? f.backups can only be accessed via an authentication mechanism outside of our corporate Active Directory	a.Yes/No YES b.Yes/No YES c.Yes/No YES d.Yes/No Daily increamental and Weekly Full e.Yes/No YES f. Yes/No YES	

S.No.	Questions	GSTN's Response	Additional Remarks
34	Are data backups regularly tested to validate the accuracy and integrity of the data and to verify the ability to restore data as quickly as possible with the least impact? If "No", kindly explain the reason	Yes/No YES	
	Cloud Security		
35	Does the organization utilize cloud based computing? If "Yes" , kindly mention the computing models used (SaaS, IaaS, PaaS, on-premises). Does the data/ application/ system/ infrastructure reside on a) Private Cloud b)Public Cloud c)Hybrid	Please specify cloud service provider name as well.	NA, Public Cloud service (IAAS) is used for E-invoice (Invoice De-Dupe System).
36	Has the organization taken measures to harden its cloud infrastructure as well as the services platform, inclusive of but not limited to identity and access management, encryption, and logging requirement to maintain the security hygiene of its cloud environment?	Yes/No/Not Applicable - Yes	Security controls (Tools, Hardening etc) are implemented in alignment with IMS policies.
	Access & Asset Management		
37	Does the organization require users remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources') : ***(Select any one)*** a. requires a valid username and password (single factor authentication) b. Multi-factor authentication is in place for some types of remote access to corporate resources, but not all c.Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented Please mention if remote access is not provided to employees	a.Yes/No YES b.Yes/No YES c.Yes/No YES	Remote access via VPN + 2FA is enabled for priviledged users. The Access is enabled for authorized users, subjected to Business Need/Approvals via PAM and monitored
38	With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together 'remote access to corporate resources'), please mention: ***(Select any one)*** a. Remote access to corporate resources requires a valid username and password (single factor authentication) b.Multi-factor authentication is in place for some types of remote access to corporate resources, but not all c. Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented Please mention if remote access is not provided to independent contractors/vendors	a.Yes/No YES b.Yes/No YES c.Yes/No - YES	Remote access via VPN + 2FA is enabled for priviledged users. The Access is enabled for authorized users, subjected to Business Need/Approvals via PAM and monitored
39	Does the organization's multi factor authentication mechanism meet the criteria that the compromise of any single device will only compromise a single authenticator? For Ex: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is kept on a device the password is also entered into, exposing both if the device is compromised	Yes/No YES	
40	Does the organization's multi factor authentication mechanism meet the criteria that the compromise of any single device will only compromise a single authenticator? For Ex: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is kept on a device the password is also entered into, exposing both if the device is compromised	Yes/No YES	
41	Has the organization implemented a centralized privileged identity and access management (PIM/PAM) solution. Please also mention number of users who have persistent privileged accounts for endpoints (servers and workstations).	Yes/No , numeric value Yes - Approx. 500 Nos	All through PAM
42	Please mention whether: a. employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented b.some of the employees are in the Administrators' group or are local admins.	a. Yes/No - YES b. Yes/No - YES	NIL Deviations to the policy
43	Does the system administrators have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.)	Yes/No YES	
44	Does the privileged accounts require multi-factor authentication and log of all privileged account usage is maintained for least the last thirty days.	Yes/No YES	
	Please specify if Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication servers/ Domain Controllers).	Yes/No NA	
45	Does the organization use Microsoft Active Directory (across all domains/forests). If yes, please specify: a. Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total) b. Number of service accounts in the Domain Administrators group: ("service account" means a user account created specifically for an application or service to interact with other domain-joined computers) Kindly mention if Microsoft active directory is not used.	Numeric value Approx. 1000	
46	Does the organization conduct periodic review of user access rights including shared accounts, privileged accounts etc.	Yes/No YES	
47	Has the organization implemented the timely removal of system access, user accounts, and associated access rights as part of the process to terminate the contract of employees, temporary employees, contractors, or vendors?	Yes/No Yes	

S.No.	Questions	GSTN's Response	Additional Remarks
48	Has the organization defined and implemented a password policy for all systems and applications with at least following parameters: a. a minimum password length of 8 or more characters b. password complexity i.e. password shall include lowercase and uppercase alphabetic characters, numbers, and symbols	Yes/No yes	
49	Does the organization has implemented information classification scheme so that all information assets are classified, handled and labelled as per its confidentiality, integrity and availability. Do you also review the handling of information reviewed on a regular basis in order to ensure consistency with its classification	Yes/No Yes	
50	Have you technically enforced the information classification scheme	Yes/No Yes	
51	Do you securely dispose sensitive information using appropriate method if it is not used any longer	Yes/No yes	
52	Does the organization ensure that the default passwords on all computer systems (e.g. routers) are changed to prevent entry in the organization?	Yes/No Yes	
53	Does the organization maintain its asset inventory for all software and hardware assets to ensure there are no poorly secured assets unintentionally left within the network?	Yes/No Yes	
54	Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions	Yes/No Yes	
55	Does the organization ensure the execution of only authorized and fully supported and updated web browsers that limit the execution of scripting language and that support only authorized plugins to minimize the attack surface and the opportunities for attacks that seek to manipulate human behavior through their interaction with web browsers?	Yes/No Yes	
56	Does the organization restrict the use of legacy (out of date/end of life) software and/or hardware that is officially not provided with security updates by manufacturers/providers (e.g. Windows XP) to prevent risk arising from legacy systems?	Yes/No Yes	
57	Is there a documented and implemented policy for cryptography and key management. Is it reviewed on periodic basis.	Yes/No Yes	
58	Does the organization have encryption requirements for data-in-transit, data-at-rest to protect the integrity of Sensitive Data including data on portable media (e.g., laptops, DVD backup tapes, disk drives, USB devices, etc.)?If "Yes", please describe where such encryption is used:	Yes/No YES	
	Does the organization has policy that all portable devices use full disk encryption?	Yes/No NA	
	Are media ports(eg. USB) managed centrally or generally deactivated	Yes/No YES	
	Physical Security		
59	Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?	Yes/No Yes	
60	Have you installed advanced entry controls (e.g. biometric access control, mantraps)	Yes/No YES	
61	Have you installed advanced entry monitoring controls (e.g. 24-7 closed-circuit television (CCTV), documentation of every access)	Yes/No YES	
	Payment Cards Related Security		
62	Does the organization collect, store, maintain or distribute credit card or other sensitive personally identifiable data?	Debit/Credit Card/Personally identifiable data (Please specify)	NA
	If "Credit Card" is selected above, does the organization comply with Payment Card Industry Data Security Standards? Also share level of requirement for PCI/DSS	Yes/No NA	
	If either is selected, is the access to such sensitive data restricted? Kindly specify who all have access to this data in the organization	NA	
63	Does the organization process payments on behalf of others, including ecommerce transactions?	Yes/No - NA	
	If "Yes" please provide the number of clients you process such payments for and an estimated number of transactions per client:	Numeric value	
	Training & Awareness		
64	Does the organization conduct general Information Security Awareness Training in every financial year for all employees to generate awareness regarding information security practices, data protection, anti-phishing, malware attack, social engineering etc. ? Whether participation records of such trainings are also maintained.	Yes/No YES	
65	Does the organization conduct simulated phishing campaigns every financial year, targeting business-sensitive employees within the organization and subsequently generate awareness to be vigilant against phishing attacks? Please mention : a. if success ratio of simulated phishing attack was less than 15% b. organization has documented process to respond to phishing campaigns	Yes/No YES	
	Incident Reporting & Analysis		
66	Does the organization has a defined Incident Response Plan (IRP) including escalation procedures. If "Yes", please mention who has reviewed and approved the document	Yes/No YES	
67	Please mention organization's average time to triage and contain security incidents of workstations year to date. The options are : a. <30 minutes b. 30 minutes - 2 hour c. 2-8 hours d. more than 8 hours	b. 30 minutes - 2 hour	
68	Is there a defined channel to report information security incident or weakness such as phone no., mail box or ticketing portal etc. which is known to employees, contractors or third parties	Yes/No YES	
69	Does the organization implement logging and monitoring of all systems or applications that process, transmit or store confidential information to identify any unauthorized security-related activities that may have been attempted or performed? Kindly also mention whether: a. server logs are stored for a defined duration b. logs are reviewed periodically c. SIEM has been implemented	a.Yes/No YES b.Yes/No YES c.Yes/No YES	-
70	Does organization conduct post incident analysis and update knowledge base to prevent incidents in future	Yes/No YES	
	Additional Security Controls		

S.No.	Questions	GSTN's Response	Additional Remarks
71	Have you implemented change management procedures for critical systems and does this includes testing, failback scenarios and reporting?	Yes/No YES	
72	Is the IT-environment for development and testing separated from production IT-environment?	Yes/No YES	
73	Does your developer do not have access to production environment	Yes/No YES	
74	Does the organization ensure that it takes effective measures for managing the security life cycle of all in-house developed and acquired software which include, but not limited to: a.secure coding practices b.using up-to-date and trusted third-party components for the software developed c. using standardized, currently accepted, and extensively reviewed encryption algorithms	Yes/No/Not Applicable YES	
75	Do you test security functionality during the development lifecycle of information systems incl. IT security updates?	Yes/No YES	
76	Are in house developed software tested prior to deployment into a production environment? If so, do they have rollback procedures in the event a failure happens once implemented into production site	Yes/No YES	
77	Do you technically or organizationally ensure that users must not install software on their workstations by themselves?	Yes/No YES	
78	Has the organization implemented measures to ensure the security hardening of applications, application servers, middleware, and databases to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes/No YES	
79	Does Any Industrial Units controlled with SCADA/DCS or any other system. If "yes", do you monitor and parser SCADA protocols in order to recognize abnormal behavior of the SCADA system / cyber events	Yes/No/Not Applicable -Not Applicable	
80	**Log 4 J queries:** 1) Does your company run or utilize any systems that are vulnerable to (CVE-2021-44228)? If Yes, have these systems been patched or short-term mitigations deployed? 2) Have you scanned your vulnerable IT systems for Indicators of Compromise (IoC) for log4shell and spring4shell and taken any necessary counter actions if needed? 3) Are you running any software that contains Apache Log4j v1 or v2 , or Java based applications? 4) What compensating controls do you have in place? 5) What is your mitigation plan? What mitigation activities have you conducted thus far? 6) Have you implemented any of the log4j scanning tools? 7) What detection measures have you put in place? 8) Have you added rules to your Web Application Firewall that prevent the possible injection text for Log4shell? 9) Have you identified your critical third parties that might be vulnerable? 10) Do you understand the scale of applications that require patching? 11) If immediate patching is not possible: Have you disabled Log4j features?	1) NA, NA 2) Yes, Yes 3) Yes 4) Patched, Perodically Scans and Audits 5) Patched, Perodically Scans and Audits 6) Yes 7) Controls at NW/Sec deviecs, application patching and Security monitoring in addition to implementation of MITRE ATT&CK Framework use cases in SOCC. 8. Yes 9. NA 10. Yes 11. NA as this is mitigated using above controls.	
	Third Party Security		
81	Has organization defined and implemented a process to select suitable third party/vendor/supplier. If "Yes", kindly explain.	Yes/No Yes	RFP process in alignment with GOI regulations
82	Does the organization outsource any part of its network, computer system or information security functions? If yes, mention the vendors/third parties to whom it is outsourced	Yes	Service providers : GSTN : Orbit GST System, Einvoice & E-WayBill - Infosys, NIC Helpdesk: Vision Plus
	If "Yes", then kindly specify: a. does the organization maintain the list of its critical third parties/vendors/suppliers b. does the Applicant periodically audit its third parties/vendors/suppliers to insure that they follow the Applicant's security policies c. track the performance of its third parties/vendors/suppliers in accordance with SLAs etc.	a. Yes/No Yes b. Yes/No Yes c. Yes/No Yes	GSTN/GST system is Certified against ISMS,ITSMS and BCMS. The certificates are valid till FY - 2026. All the policies/process etc are aligned with the same.
83	Does the organization require indemnification from Outsourcers for any liability attributable to them?	Yes/No Yes	
84	Does the organization contractually require all Outsourcers to comply with the terms of the organization's data protection and Information Security policies?	Yes/No Yes	
85	Does the organization perform a cybersecurity risk assessment prior to conducting business with all third-party vendors and a continual assessment every financial year to identify if all their third-party security requirements are met?	Yes/No Yes	
	BCP and Disaster Recovery		
86	Does the organization has a documented Business Continuity Plan (BCP) which is tested periodically(Attach Copy of BCP) . Also mention frequency of BCP testing.	YES	
87	Has the organization conducted Business Impact Analysis (BIA) in last 12 months. If "Yes", please mention maximum acceptable outage or also known as RTO (Recovery Time Objective) for mission critical systems : a. <4 hours b. 4-24 hours c. 1-2 days d. 2-7 days	Yes < 4 Hrs	
88	Does the organization has a documented Disaster Recovery (DR) Plan and how often DR drill is conducted to ensure the effectiveness and efficiency of its disaster recovery plan? (Attach copy of DRP)	Yes/No Yes	
89	Does the organization ensure a high availability of business critical infrastructure to ensure business continuity in case of an incident?	Yes/No Yes	
	Also mention, if organization tests its ability to restore different critical systems and data in a timely fashion from its backups at least twice a year	Yes/No Yes	

S.No.	Questions	GSTN's Response	Additional Remarks
90	What redundancies are leveraged in the design of your infrastructure ? (E.g., automatic failover logic, multiple processors, redundant I/O modules, Dual trinked networks)?	Yes/No Yes	HA with automatic failovers
91	What kind of redundancies do you leverage for your mission critical systems? Are you on a hot or warm site standby?	Yes/No Hot	
92	Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of a disaster?	Yes/No Yes	
	Ransomware		
93	Are anti-ransomware toolsets deployed throughout the organization	Yes/No - Yes	
94	When was the last ransomware exercise was performed in the organization. Kindly also mention if organization has documented plan to respond to ransomware of a 3rd party provider/vendor or customer	NA	
95	What proactive measures are in place for identification of ransomware threats – extent of the damage, attack vector, downtime, threat of a related data breach etc. (including any red teaming exercise)?	External VA/PT, Red Teaming etc	
96	Does the organization has in-house capabilities or external arrangements in place to spot the symptoms of ransomware, analyze and identify ransomware strain used and take appropriate actions ?	Yes/No Yes	
97	Please specify whether: a. organization has Breach and Attack Simulation (BAS) software to verify the effectiveness of security controls b. internal "red team" that tests security controls and response c. engaged an external party to simulate threat actors and test security controls in the last yea	a. Yes/No No b. Yes/No YES c. Yes/No Yes	
	Claims information		
98	In the past five years, has organization suffered any security breach, failure of hardware or software systems, intentional damage or attempt to damage or corrupt applications or data, or had a software or hardware malfunction that affected the whole or part of the organization's critical systems, resulted into business disruption. Please mention when was it occurred.	NO	
	If the answer to the above question is yes, how many incidents did the software or hardware malfunction cause the network (or any portion thereof) to stop operating totally or failed to start operating without any human intervention?	<Numeric Value e.g. 3>	
99	In reference to above question, please mention: a.primary causes of the hardware or software malfunctions b. total cost incurred (not including standard staff time and other regular operating expenses) to rectify the malfunction and bring the critical system(s) back online	NA	
100	Has the organization encountered a security breach that required notifications to customers or other third parties?	NA	
101	Please mention the measures taken by the organization to prevent the reoccurrence of the issue/ breach faced	NA	
102	What actions did the organization take to recover the applications, data, or cost of recovery and how long it takes to restore the affected applications/ operations?	NA	
103	Please specify: a.If organization ever been refused for cybersecurity or similar insurance, or had a similar policy cancelled b. Does the organization currently have cyber security or similar insurance? Please enter the limits and other details of the insurance.	NA	
	Declaration		
	1. I/we herby confirm that all premiums have been/will be paid from bonafide sources and no premiums have been/will be paid out of proceeds of crime related to any of the offence listed in Prevention of Money Laundering Act, 2002. 2. I understand that the organization has the right to call for documents to establish sources of funds. 3. The insurance organization has right to cancel the insurance contract in case I am/ have been found guilty by any competent court of law under any of the statutes, directly or indirectly governing the prevention of money laundering in India.		