

CORRIGENDUM NOTICE**Corrigendum to bid document for e-tender for Cyber Crime Insurance policy
(Tender published of GeM portal)**

In Ref no. **GEM/2024/B/4906934** dated 02.05.2024, we hereby notify responses for the queries raised by prospective bidders through this corrigendum to all concerned.

Company Information:

1. Name: GENERAL INSURANCE CORPORATION OF INDIA
2. Address : “SURAKSHA”. 170 J TATA ROAD, CHURCHGATE, MUMBAI, 400020, INDIA.
3. Date established: 22nd November 1972
4. Principal activities/services : Reinsurance
5. Number of directors : 6 Directors
6. Number of employees:
 - (a) Domestic : 407
 - (b) Overseas : 25
7. Number of locations:
 - (a) Domestic: Head Office, One branch office in Gift City & 1 Liaison Offices (Delhi)
 - (b) Overseas: 3 Branches and 2 Subsidiaries
8. Web site: www.gicre.in

9. Geographical Exposure:

Particulars	Previous Year (FY 22-23)	Current Year (Upto 31 st Dec 2023)
Total Gross Revenue	Rs 36,591.59 Crore	Rs 28,458.11 Crore
Geographical Split of the Company's Total Gross Revenue (%)		
European Union	4.45%	3.88%
United States	3.17%	8.94%
Rest of World	92.38%	87.18%

10. Brief details of loss during the past 5 years as follows:

Nature of Loss	Date of Discovery	Location	Amount of Loss
Cyber Fraud by the outside entity	13th April 2022	GIC Head Office	USD 326,500.70

(Sd)
CISO

Response to Queries- Security parameters - Reference: GeM Portal Bid Ref:GEM/2024/B/4906934

SI No	Queries	Response
1	Does the company have Board approved Information Security & privacy policy and it is communicated to all stakeholders?	Policy is in place and communicated to all stakeholders
2	Does the company have Board approved Incident Response Plan, Disaster recovery plan, Business Continuity plan and are they reviewed at least annually?	Approved Disaster recovery plan, Business Continuity plan are present and are reviewed Annually
3	Which are the information security certification hold by your organization?	GIC complies to ISO 27001 security guidelines.
4	Does the Company conduct regular Review/Audit of the consultant and third party service providers to ensure that they meet the company's requirement for critical data in their custody?	Audit/Review is conducted at least once a year
5	Does it require to comply with data protection laws applicable to jurisdictions in which company operates?	IT Act 2000, Govt. of India
	IT system security	
6	Are security audit logs generated for all hardware and software's installed on it?	Yes
7	What is the frequency of validation of log reports to uncover the anomalies of Critical System Components?	At least weekly
8	Are only fully supported/updated web browsers and email clients allowed to execute in the organization?	Yes, email client and web browser are regularly updated
9	Is secure configuration is used for all software's and hardware (Mobile devices, Laptop, Workstations and servers) including network devices (firewall, router and switch)?	Yes
10	How often assessment programs run to determine whether all systems' software's & security patches are updated?(including remote access connection)	Continuous assessment Program is scheduled
11	Does company have Anti virus & Firewall installed on on computer system? If yes, What is the frequency for updating this?	Updated daily
12	Is comparison of firewall, router and switch configuration against standard for each network devices performed?	Yes
13	Is cyber security assessment performed for all applications before moving into production?	Yes
	Network Security	
14	Is any network access control technology in place to authorize authenticated devices and software installation before allowing them on the network?	Network Access control for both Authenticated Software and Devices
15	How often all the Ports are scanned against all critical servers for to & fro data movement ?	Monthly Scans
16	Does the company have checks in place to identify and detect network security weakness? (internal/External Vulnerability assessment)	Yes
17	Does the Insured have End point Solutions in Place ?	Yes
18	Does the Insured have a Behavioral based end point?	Yes
19	Any external or internal penetration tests are conducted to identify vulnerabilities or attack vectors? If yes, What is the frequency of penetration tests	At least Quarterly
20	In case of cyber attack, which multilayer boundary defense are in place to filter inbound and outbound traffic(including business partner network)? Multiple Choice	NGF(Next gen firewall)/web application firewall
	Data Security	
21	Which type of data organization collect, store & process? (Multiple Choice)	Business(corporate Info)
22	What is the frequency of Data Back Up(Operating System, Application Software and Data)?	Weekly

23	Has your organisation undertaken a Phishing Campaign on Periodic basis	Yes
24	How many times data restoration process is verified to ensure back up data is properly working?	Quarterly
25	Is data in stored form(On Cloud, Servers,Laptops,flash drives, back up tapes) or in transit form, encrypted using strong encryption technologies?	Data in stored form only is encrypted
26	Are data access restrictions enforced on the basis of specific role rights ?	Yes
Access Management		
27	How many times Admin access rights are reviewed to ensure only that only administrative functions (Non-Internet Connection based) are performed on those systems?	Fortnightly
28	Which user access management methods are being used in your organization? (Multiple Choice)	Strong Password policy with unique, complex & with expiration date
29	Does company have security controls in place to authenticate all user(including remote user and wireless area) before being allowed to connect to internal network and computer system?	All users are authenticated before connect to network
30	Does the Insured have a VPN 2 factor authentication if connecting from a external network?	Yes
31	Is each user provided with unique user ID on the system and network level?	Yes
32	Does the organization conduct and measure general Information Security Awareness Training in every financial year to ensure all employees are aware of their responsibility towards information security and the cyber threats they might be susceptible to?	Yes
33	Does the organization conduct simulated phishing campaigns every financial year, targeting business-sensitive employees within the organization and subsequently provide training for preparing employees to be more resilient and vigilant against phishing attacks?	No
34	Does the organization conduct domain-related security training tailored to specific roles for all employees (including senior management) in every financial year to ensure all employees are implementing effective cybersecurity concepts in their specific domain?	Yes
35	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?	Yes
36	Does the organization have network segregation implemented by isolating the demilitarized zone, Management VLAN, and Guest VLAN to prevent the movement of an attacker in case of a breach?	Yes
37	Does the organization perform regular backups of business-critical data on servers to recover such data in cases of breaches, like ransomware attacks?	Yes
38	Does the organization ensure backups are 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?	Yes
39	Does the organization perform Incident Reporting, Investigation and Recovery effectively to ensure the recurrence rate of security events is minimal?	Yes
40	Has the organization implemented the 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
41	Does the organization conduct regular external penetration tests and red-teaming exercises to test organizational readiness for identifying/ responding quickly to vulnerabilities/attacks?	Yes
42	Does the organization create dedicated accounts with unique passwords for all personnel with privileged access to help separate internet risks (phishing attacks, web browsing) from privileged access accounts and to mitigate the risk of an adversary abusing stolen hashes for attacking other computers?	Yes

43	Does the organization perform regular backups of business-critical data on endpoints and ensure such backups are regularly tested to validate the accuracy and integrity of the data and their ability to restore data as quickly as possible with the least business impact in case of an attack on the availability of data, like with ransomware?	Yes
44	Does the organization timely, i.e. at least monthly, update IT systems and applications to prevent any known vulnerabilities being exploited?	Yes
45	Has the organization implemented a password creation policy with a minimum password length of 8 or more characters, including lowercase and uppercase alphabetic characters, numbers, and symbols, for all systems and applications to ensure that passwords are harder to break?	Yes
46	Does the organization ensure that the default passwords on all computer systems (e.g. routers) are changed to prevent entry in the organization network through a brute-forcing attack?	Yes
47	Does the organization ensure effective disposal methods, like shredders, are used for properly disposing of confidential information in order to prevent attacks originating from information gathered by activities like dumpster diving?	Yes
48	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?	No
49	Does the organization ensure that it takes effective measures for managing the security life cycle of all in-house developed and acquired software, like establishing secure coding practices appropriate to the programming language and development environment being used, only using up-to-date and trusted third-party components for the software developed by the organization, and only using standardized, currently accepted, and extensively reviewed encryption algorithms, in order to prevent, detect, and correct security weaknesses?	Yes
50	Does the organisation ensure a high availability of business critical infrastructure to ensure business continuity in case of an incident?	Yes
51	Does the organization have a Disaster Recovery (DR) site to allow it to continue business-sensitive operations in the event of a disaster?	Yes
52	Has the organization performed a Disaster Recovery (DR) drill to ensure the effectiveness and efficiency of its disaster recovery plan?	Yes
53	Does the organization identify and mitigate vulnerabilities and configuration flaws through security assessments conducted at least every financial year?	Yes
54	Does the organization have a dedicated Network Operations Center (NOC) that is capable of monitoring, reporting, investigating and recovering any security incident observed within the organization's network?	Yes
55	Has the organization documented and implemented a cloud security policy to ensure security requirements are catered to when utilizing cloud services for business?	Yes
56	Has the organization implemented security hardening of its network and security devices to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes
57	Does the organization implement encryption for the transmission and storage of sensitive and confidential information per the relevant compliance requirements of the organization to prevent breaches of confidential information in the event of a device compromise?	Yes
58	Has the organization implemented strong authentication protocols for wireless networks to prevent wireless security attacks?	Yes
59	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

60	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
61	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
62	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
63	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
64	Has the organization implemented security hardening of its end-user systems and servers to reduce the attack surface, giving attackers fewer opportunities to gain a foothold within your IT ecosystem?	Yes
65	Has the organization implemented active and passive network discovery solutions capable of rogue device detection within their network so that only authorized devices are given access, while unauthorized and unmanaged devices are found and prevented from gaining access?	Yes
66	Does the organization have a Network Access Control (NAC) solution in place to allow the organizations to restrict access to resources on their network and to prevent risk to the organization from Bring Your Own Device (BYOD), the internet of things (IoT), weak access permissions, and advanced persistent threats (APT)?	Yes
67	Has the organization implemented an Enterprise Threat Protection (ETP) DNS proxy to detect and prevent any malicious activity ingress to the organization?	Yes
68	Has the organization implemented a Deception Tools & Honeypots solution to divert and detect attackers with no risk to real data, operations, or users?	Yes
69	Has the organization implemented host-based firewall solutions on end-user devices and servers to actively identify and mitigate malicious traffic incoming to and outgoing from assets?	Yes
70	Has the organization implemented an Advanced Persistent Threat (APT) solution on end-user devices and servers to actively monitor and detect security threats based on system behavior?	Yes
71	Has the Organisation implemented EDR solution? Please specify which one has been implemented?	Yes
72	Does the Insured have a Behavioral based end point? Is the End point security implemented in both prevention and detection mode?	Yes
73	Has the organization implemented an application whitelisting solution on end-user devices and servers to limit the use of only authorized licensed applications on the assets?	Yes
74	Has the organization implemented a User Entity Behavior Analysis (UEBA) solution on end-user devices and servers to detect anomalous behavior and to prevent insider threats/compromised users?	Yes
75	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
76	Has the organization ensured that the standard security configuration of internal firewalls is individually adapted to prevent access to unauthorized external websites?	Yes
77	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
78	Does the organization have a Next-Generation Firewall (NGFW) or Unified Threat Management (UTM) solution capable of in-line Deep Packet Inspection (DPI) and an Intrusion Prevention System (IPS) in place to reduce risks arising from network vulnerabilities?	Yes

79	Does the organization ensure only secured connections are utilized for remote users to ensure the confidentiality of sensitive information in transit?	Yes
80	Has the organization implemented a Security Incident and Event Management (SIEM) solution for proactively preventing, detecting, analyzing, and responding to security threats that the organization may face in a timely manner?	Yes
81	Has the organization implemented a centralized privileged identity and access management (IAM) solution to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications?	Yes
82	Has the organization implemented a Mobile Device Management (MDM) solution to monitor, manage, and secure employee's mobile devices?	Yes
83	Has the organization implemented a Database Activity Monitoring (DAM) Solution to detect and prevent malicious behavior in the database?	Not Applicable
84	Has the organization implemented a Network Behavior Anomaly Detection (NBAD) solution to continuously monitor the network for unusual events or trends that indicate a threat to the organization?	Yes
85	Has the organization implemented a Web Application Firewall (WAF) capable of preventing the exploitation of web application vulnerabilities covering at least OWASP's Top 10 threats?	Yes
86	Has the organization implemented a host-based intrusion detection and prevention solution (HIDS/HIPS) on end-user devices and servers to detect and prevent any malicious activity on assets?	Yes
87	Has the organization implemented a Configuration Management Solution (CMS) to conduct regular configuration security assessments on all organization-owned assets?	Not Applicable
88	Has the organization implemented a Load Balancer to maintain the availability of critical resources?	Yes
89	Has the organization implemented anti-Distributed Denial-of-Service (DDoS) solutions to prevent DDoS attacks?	Yes
90	Has the organization implemented a Vulnerability Management Solution (VMS) to conduct regular Vulnerability Assessment and Penetration Testing (VAPT) security assessments on all organization-owned assets?	Yes
91	Has the organization implemented a patch management solution to ensure that all critical and high-risk vulnerabilities reported are patched or mitigated within two days?	Yes
92	Has the organization implemented anti-malware or equivalent protection on end-user devices and servers that are updated/patched as per the vendor's recommendations to prevent malicious software attacks (e.g. IT virus, ransomware, spyware, etc.)?	Yes
93	In the past five years has anyone intentionally damaged or corrupted, or attempted to damage or corrupt applications or data, or had a software or hardware malfunction that caused the whole or part of the organization's critical systems, failed to start/ stop operating, or had a breach?	No
94	How long did the organization take to restore the affected applications/ operations?	It is depend on the application. We maintain 15 minutes of RPO.
95	Please provide comments on the exposure of Proprietary & Confidential data that the organization host, store, share, transmit, publish, or transact.	NA
96	Please provide comments on the exposure of published electronic content.	Corporate Website
97	Has the Security Incident Response Plan been reviewed and approved by the organization's Board of Directors or persons with substantially similar responsibilities?	Yes
98	Has the organization ever been refused for cybersecurity or similar insurance, or had a similar policy cancelled?	No
99	Does the organization currently have cyber security or similar insurance? Please enter the limits and other details of the insurance.	Yes
100	Does the organization conduct a test for the IT Security Incident Response Plan	Yes

Response to Queries- Data Centre Controls - Reference: GeM Portal Bid Ref:GEM/2024/B/4906934

Technical / Process Controls	Queries	Response
Cloud Exposure	What is your cloud adoption status ?	Microsoft 365, GCC (Govt of India initiative)
	Are any SAAS services being used or provided? IF yes, who is responsible for the protection of data stored on the SAAS service?	No
	Have the cloud service provider(s) undergone any third party cloud security assurance or certification (example: ISO/IEC 27001/27002:2022, ISO 27018, IRAP, SOC 2 etc.) (Cloud Security Certification) ?	No
	Does your cloud environment follow the cloud security standard laid by PCI DSS for use of cloud technologies and considerations ?	Yes
	Do you have 3rd party vendors accessing your network? How many inbound and outbound APIs do you have?	No
	Do you evaluate the inbound and outbound APIs for OWASP Top 10 API Security Risks ?	No
	Do you use an automated/manual source code analysis tool to detect security defects in code prior to production? (Application & Interface Security)	No
	Is multi-factor authentication enabled for the root account access?	Not applicable
	Have you implemented Cloud security posture management (CSPM) to continuously monitor compliance and visibility into cloud infrastructure?	Not applicable
	Is the cloud log integrated with SIEM for 24*7 monitoring ?	Yes
	Please elaborate any other measures taken from cloud security perspective	
Outsourced Service Providers	CtrlS Data Center	Data Center and Disaster Recovery Site
Vendor Management	How many third parties, including number of organizations and number of individuals from vendors and subcontractors, have access to internal systems (e.g., virtual private network, modem, intranet, direct connection) ?	2
	Have you deployed - Vendor Categorization ?	No
	Do you conduct onboarding assessment and annual assessment for vendors ?	Yes
	Does your contract with vendors capture the escalation matrix of vendors which gets reviewed annually. ?	Yes
	Is there a documented Third party security policy to ensure the implementation security controls with respect to the services provided by the Third Party.?	Yes
	Do you document the changes in the services provided by the third party in the maintenance and support contract.	Yes
	Do you perform risk assessment whenever there is change in the service provided by the third party and appropriate actions are taken for the closure of identified risks.	Yes
	have you enforced appropriate risk-based multifactor authentication (MFA).?	Yes
	How do you handle access management (provision/modification /revocation) for vendors ?	It is based on the request and approval from appropriate authority

	Do you have provisions for compliance with applicable regulations (SOX, HIPAA, PCI)		NA
	Do you have the clauses for - Right to audit, Right for Data management etc. in vendor contracts ?		NA
	Do you have the clauses for Liability Capping and Indemnification in in vendor contracts ?		NA
Network Controls	SOC Setup	Is your SoC setup In-house or Outsourced	Outsourced
		Please confirm if network security logs are monitored across all critical systems with 24*7 SOC monitoring	Yes
		What is the scope of SOC monitoring i.e. do they monitor entire network including logs & events from users, cloud, apps, servers and workloads, networks, endpoints etc.	Entire network including logs & events from users, cloud, apps, servers and workloads, networks, endpoints etc
	Are firewalls in place at all external connection points?		Yes
	Please confirm on internal network segregation (VLAN, Micro, DMZ) .		Yes
	Please let us know if there is segregation based on geographies and business divisions to avoid any lateral spread of malware		NA
	How frequently do you review firewall rules, configurations and settings (quarterly/monthly/annual/biannual etc.) ?		Quarterly
	What is the scope of the VA and PT (Web,Mobile,IT Infra/Network/API/ OT/ICS/SCADA/DCS)		Web,Mobile,IT Infra/Network
	What is the Frequency of VA and PT (quarterly/half yearly/Annually)		Quarterly
	Please confirm if finding in last VAPT have been patched. (if not please provide roadmap)		Yes
Logging & Monitoring	What is the scope for SIEM (network traffic, Endpoint data, System log, System Event, User Analytics, cloud log)		Network traffic, Endpoint data, System log, System Event,
	How are the resolution rules for SIEM updated i.e. is it manual or automated		Automatic
	What is the scope of SIEM – Does it cover all endpoints / only the exposed ?		Security Information and Event Management: SIEM collects security data from network devices, servers, domain controllers, and other log sources.
Patching	Does the Company have written patching policy in place with explicit mention to Critical, Important and normal patches with timelines for their implementation		Yes
	Are there any unmanaged devices which are connecting to the network?		No
	Does the patching process manual or with Automated tool		Automatic
	What are the set timelines for Critical patches		On immediate basis
Endpoint Security	What are the security solutions deployed at End Point ?		DLP for all endpoints, Email & Web (Arcon & M365)
	a) Standard Anti-virus [McAfee MVISION/Symantec/Microsoft Defender/Webroot Endpoint Security...etc.]		Microsoft Defender
	b) Next-Gen Anti-virus [CrowdStrike Falcon Protect/Sentinel One Singularity Core/Sophos Intercept X Advanced. Etc.]		Next-Gen Anti-virus

	c) Endpoint Detection & Response [CrowdStrike Falcon Insight/Sentinel One Singularity Complete/Sophos Intercept X Advanced with XDR/FireEye Endpoint Security/Microsoft Defender for Endpoint..etc.]		Endpoint Detection & Response	
Remote Connectivity	Remote Connectivity Type		MFA in Place? (Yes / No)	What is 2nd factor in use? (e.g. OTP, Call and Authenticator)
	VPN		Yes	All three
	Email over Internet		Yes	All three
	Infrastructure hosted in Cloud		Yes	All three
	Please confirm on No remote connectivity solution exposed to internet without MFA		NO	
	Please confirm on Remote Desktop Protocol (RDP) is disabled or it must be accessed from behind a firewall, through a VPN configured for network-level authentication, and/or the IP addresses of all authorized connections are whitelisted.		YES	
Access Control	Confirm on Whether Company conduct detailed, Access control and User account review for all user accounts and frequency of this review		Yes	
Privilege Access	1) Administrative users use different accounts for administrative use and non-administrative use (e.g. day to day activities) 2)Standard users do not have administrative rights to their workstations 3) Local administrator accounts are unique and complex on all systems 4)A password management vault is used to manage privileged accounts		Administrative users use different accounts for administrative use and non-administrative use (e.g. day to day activities)	
Email Security	Sender Policy Framework (SPF)		Yes	
	DKIM (DomainKeys Identified Mail)		Yes	
	Domain-based Message Authentication, Reporting and Conformance (DMARC)		Yes	
	Are email gateways configured to look for potentially malicious links, programs, and block executables?		Yes	
Data Management	Encryption solutions	Data at rest	Yes	
		Data in transit	Yes	
		Network (network level encryption)	Yes	
		Endpoint devices (Laptops, tablets and removable media)	No	
	Data Loss Prevention (DLP)	Do you have a Data Loss Prevention (DLP)	Yes	
		What is the scope of DLP (Network/Endpoint/Email/Cloud) ?	email	
Backup	Are backups encrypted?		Yes	
	Is there a process in place for successful restoration and recovery of key assets within the RTO?		Yes	
	Are backups periodically retrieved, compared to the original data to ensure backup integrity?		Yes	
BCP and DR	Does the BCP plan include impact of a cyber incidence on Business Operation ?		Yes	
	Does the BCP plan has defined BIA and RTO for all critical operations ?		Yes	
	What is the maximum acceptable outage or also Known as RTO (Recovery Time Objective) for Critical system and RPO (recovery point objective) ?		RTO -1 Hour; RPO 15 Minutes	
	Does the Company have DR Site to continue business operation in the event of disaster		Yes	
	Which kind of disaster recovery sites is being used: cold, warm, and hot sites ?		Cold	
	What is the frequency of IT DR drills		Twice in year	
	How is the DR set-up done ? Is it Active-Passive or Active-Active ?		Active-Passive	
	If it is active passive set up, what is redundancy (failover time) ?		real time replication	

	If it is a active set up how does orchestration happen ?	online replication
Software Development [Applicable for companies who have inhouse application development capability or have outsourced their customization and development of application to a 3rd party]	a. Do you perform threat modelling for Secure Software Development ?	NO
	b. Do you test the application developed for the OWASP® Foundation's top 10 vulnerability list ?	NA
	c. Do you test the software development lifecycle as per the critical controls laid by Centre for Internet Security (CIS) ?.	No
	d. Do you ensure Secure Software Coding practices are followed ? If yes , please provide details	No
	e. If WAF(s) is deployed, does the web application firewall inspect all traffic?	Yes
	f. Do you ensure code review is performed regularly to ascertain and identify potential security issues? ? If yes , please provide details	NA
	g. Do you have regular security testing (including penetration testing and vulnerability scanning) to help identify potential security weaknesses in the software development ?	Yes
	h. Do you ensure regular software updates and patches are applied to help address security vulnerabilities and reduce the risk of security breaches ?	Yes