Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
1	Eligibility Criteria	10	The OEM should be a Software Development, IT Application & Maintenance company registered/ incorporated under Indian company Act and must have 10 years of existence in India as on date of submission of bids.	We kindly request the Authority to consider OEMs with less than 10 years of existence as eligible, provided they have successfully executed similar projects, hold relevant industry certifications, maintain an established support and service organization in India, and can demonstrate the maturity, reliability, and proven track record of their proposed product through satisfactory customer references.	No change in RFP.
2	Eligibility Criteria	11	OEM should have average annual turnover of INR 300 crore in the past three financial years in India.	We kindly request the Authority to consider providing relaxation in the stipulated average annual turnover requirement of INR 300 crore during the preceding three financial years. This relaxation would enable more Make in India OEMs with proven experience, strong technical capabilities, and demonstrated expertise in delivering similar solutions to participate in the opportunity. It would help ensure wider participation from technically capable and experienced OEMs, irrespective of their overall turnover scale.	No change in RFP.
3	TABLE A:- Specifications/Features Point No. 44	5	File integrity monitoring should be implemented in order to ensure authenticated changes and to detect unapproved changes to files.	Kindly clarify if you are looking for an integration with FIM Solution or the SIEM solution to have native capabilities of FIM.	The proposed SIEM solution should have native File Integrity Monitoring (FIM) capabilities to detect and monitor unauthorized changes to critical files, configurations, and system components.
4	6.2. Project Timelines	42	The time period required for the completion of the SIEM solution implementation activities(30 days)	Considering the buffer scenario, the delivery is taking longer than anticipated; to prevent project delays and ensure smooth processing please provide minimum 45 days extension to the delivery schedule.	Depending on the implementation scenario and challenges encountered, an extension of the implementation period may be considered post on boarding of successful bidder and as mutually decided. However, there shall be no change to the commercial/billable implementation period.
5	-	-	-	Kindly requesting you to provide the exact EPS sizing details for the proposed SIEM solution.	Please refer to the corrigendum.
6	Appendix-1B- Technical- Specifications Licensing and implementation requirements Point No. 1	10	The solution can be put to use at NABFINS, NABFINS branches, Subsidiaries and associates (current and future)	Kindly confirm if any remote locations are present for the logs to be collected.	The scope includes NABFINS Head Office infrastructure, along with integrations, consoles with cloud-based infrastructure and SaaS applications.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
7	6 Scope of work Appendix-1A-SIEM-Functional SIEM_025	16 2	Bidder shall store all logs for a minimum period of one year. Preferably, logs for 1–2 months shall remain online, after which they may be moved to archival storage Minimum 365-Day Online Log Retention	There is a discrepancy in both cases, kindly give more clarity on, Online retention is for 1 to 2 months or for 365 days? Also, please provide the archival time period for the same	Please refer to the corrigendum.
8	Eligibility Criteria – Page 11 - Point 11	12	"The bidder should have experience SIEM project in BFSI/PSU/PSE/Govt. Organization in India within last 03 years as on the date of bid opening."	We request NABFINS to clarify whether OEM's SIEM project experience in BFSI/PSU/PSE/Govt. can be considered valid when the bidder is an authorized partner of the OEM. Megamax Services, as an authorized partner, proposes to leverage OEM's proven SIEM credentials.	The Bidder should have experience in implementing SIEM projects for BFSI/PSU/PSE/Government organizations in India within the last three years as on the date of bid opening.
9	Eligibility Criteria – Page 11 - Point 11	12	"The bidder should have experience SIEM project in BFSI/PSU/PSE/Govt. Organization in India within last 03 years as on the date of bid opening."	Kindly confirm if NABFINS will allow consortium/partnership bids where the OEM provides SIEM expertise and Megamax Services acts as prime bidder for compliance, project management, and integration.	No change in RFP.
10	Eligibility Criteria – Page 11 - Point 11	12	"The bidder should have experience SIEM project in BFSI/PSU/PSE/Govt. Organization in India within last 03 years as on the date of bid opening."	We request relaxation to allow equivalent IT services /compliance projects in BFSI/PSU/Govt. to be considered in place of direct SIEM experience. As if OEM confirms multiple SIEM deployments in BFSI/PSU/Govt. Kindly clarify if OEM's credentials can be considered sufficient when the bidder is an authorized partner, with end to end commiments	No change in RFP.
11	Manpower Requirement (Point 8)	11	The bidder should have at least 50 Functional/ IT Professionals on its payroll as on the date of bid opening date.	We request NABFINS to clarify if consortium arrangements or subcontracting can be considered to meet the manpower requirement,	No change in RFP.
12	Clause 10.8 & 10.9	Pg 71 & 73		Clause 10.8 states that "Bidder (L1) quoting the lowest bid will be selected on the basis of Total Price post commercial bid evaluation" whereas clause 10.9 elaborates on Final evalaution as QCBS evaluation (70:30). We understand that the selection criteria would be QCBS (70:30). Kindly confirm.	Please refer to the corrigendum.
13	Section 5, Point 11, Eligibility Criteria	Pg 12	The supporting documents sought against this criteria are 1. Copy of 'Contract/Purchase order' 2. Confirmation/credential/email from client on having executed/executing the PO.	Requesting to please amend this criteria to 1. Copy of 'Contract/Purchase order/Agreement/SoW' 2. Self declaration from the bidder regarding the engagement. Obtaining completion certification from client at such a short notice is a challenge. Requesting to kindly consider the amendment.	Submission of completion certificate is desirable. However, submission of a copy of the valid Purchase Order (PO) will be considered.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
14	Annexure 18, Existing Infrastructure and solution details	Pg. 122		Request NABFINS to share indicative current log volume data (EPS, GB/day, or historical monitoring data) before bid submission to enable accurate sizing. This information is critical and will allow all bidders to be evaluated equally on sizing adequacy.	Please refer to the corrigendum.
15	Annexure 18, Existing Infrastructure and solution details	Pg. 122	Aadhaar Data Vault: 3 units listed as in-scope log source for SIEM integration.	Clarification sought (a) Does SIEM log ingestion from the Aadhaar Data Vault require data masking, tokenization, or anonymization of Aadhaar numbers prior to log transmission to the SIEM? If yes, is this the vendor's or NABFINS's responsibility? (b) Does ingesting Aadhaar Data Vault logs into a cloud-hosted SIEM require prior UIDAI approval or NOC? Has NABFINS already initiated this? (c) What log types are expected - audit/access logs only, or operational/transaction logs? This determines masking requirements and retention treatment.	(a) Confidential data such as Aadhaar numbers, Voter ID numbers, etc., need not be captured, and no data masking is required. (b) NABFINS will initiate the necessary actions. (c) The relevant details will be shared with the successful bidder.
16	6.2 Project Timelines (Table, S.No. 5 & 8)	42	"S.No 5: VAPT (Solution) & IS Audit (Solution and Infra) [Start: T0+10, End: T0+15 days] ... S.No 8: Go Live, Knowledge Sharing [Start: T0+20, End: T0+30 days]	Timeline Revision & Third-Party Audit Risk: Achieving Go-Live in 30 days including a full-scope VAPT and external Information Security (IS) Audit is extremely high-risk. IS Audits rely heavily on external certified auditors, regulatory frameworks, and NABFINS's internal scheduling. Any external delay represents a critical project blocker beyond the bidder's control. Additionally, A 30-day go-live is extremely high-risk for an end-to-end SIEM deployment covering approximately 15 infrastructure components, especially if custom parsers are required. We request either: 1. Extending the timeline to 60 days.2. Decoupling the Go-Live date from formal third-party audit completion.3. Allowing a phased ingestion approach (Phase 1: Core SaaS/Cloud logs; Phase 2: Custom/FinTech sources).	1.Certain log source integrations may depend on external vendors. In case of delays or challenges from such vendors, NABFINS may consider an extension to the go-live timeline, subject to the circumstances. 2.Third-party audits may be initiated in parallel with the implementation activities. 3. Once onboarded, the bidder may discuss and finalize the detailed integration approach with NABFINS.
17	6.1 Cloud and CSP Requirements (Point f)	21	"Bidder should arrive at the sizing independently. In case, the sizing quoted by the Bidder fails to meet the necessary services, NABFINS will not bear any cost for upgrades or replacements..."	Request for Log Ingestion Sizing Metrics: To perform accurate data sizing and avoid penalties for capacity shortfalls, bidders need objective telemetry. Please provide the daily log ingestion volume in Gigabytes per Day (GB/day) or the average/peak Events Per Second (EPS) across all 15 systems listed in Annexure 18	Please refer to the corrigendum.
18	13.2.18 Annexure 18: Existing Infrastructure	122	"S.No 1: AWS Cloud Watch... S.No 3: Zoho Cloud Platform... S.No 4: HSM... S.No 5: ADV (Aadhaar Data Vault)"	Clarification on API Access & Custom Parsers: 1. Please confirm if standard log access APIs/feeds are fully enabled for the cloud-hosted AWS and Zoho platforms.2. For localized Indian FinTech systems like Aadhaar Data Vault (ADV) and HSMs, please clarify if raw schema samples will be shared during the SRS stage to facilitate custom parser creation.	The details will be discussed with the successful bidder.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
19	6.1 Detailed Scope of Work (Clause m)	18	"Preferably, logs for 1–2 months shall remain online, after which they may be moved to archival storage."	Technical Scoring Favorability for Online Storage: Cloud-native SaaS platforms like Google SecOps keep all 12 months of log retention as "hot/online" (instantly searchable in milliseconds) rather than moving them to slow cold archives. Please confirm if proposed solutions offering 12 months of hot/online storage out-of-the-box will be scored favorably under the Technical Bid Evaluation (Section 10.7).	Please refer to the corrigendum.
20	Appendix 1B (S.No. 78 & Table B Section ss)	8 & 10 (App 1B)	"The application and DB is/will be hosted separately on a dedicated instance for NABFINS... Shared database services should not be used, database, clusters and all other resources must be setup separately for NABFINS."	Request to Accept Logical Segregation: True cloud-native, SaaS-based SIEM solutions run on highly secure, logically isolated multi-tenant architectures. We request that strict logical segregation, secure workspace isolation, and dedicated Customer-Managed Encryption Keys (CMEK/BYOK) be accepted in lieu of physically dedicated servers and databases	Please refer to the corrigendum.
21	Appendix 1B (S.No. 9 & 69d)	2 & 7 (App 1B)	"The bidder should provide CSP's third-party audit reports on... Source code review including APIs... Every year irrespective of any audit on demand.	Clarification on Source Code Audits: Hyperscale cloud providers do not share proprietary platform source code. We request that industry-standard independent security certifications (such as SOC 2 Type II reports, ISO/IEC 27001, and OEM penetration testing summaries) be accepted in lieu of a direct source code review of the CSP's backend platform.	The SIEM OEM need to have conducted a source code audit. The audit report shall be submitted to NABFINS for compliance verification.
22	Appendix 1B (S.No. 20)	3 (App 1B)	"Bidder to perform backup on a daily basis and half-yearly back-up restore tests in presence of NABFINS staff."	Clarification for SaaS Backup/Restore: Since cloud-native SaaS SIEMs feature active-active regional replication and native high durability with no traditional database restoration tasks, please confirm if half-yearly DR failover validations or configuration export/import tests satisfy this requirement.	For compliance purposes, half-yearly Disaster Recovery (DR) failover validation shall be conducted. A Database Restoration Test shall also be performed to verify that backups can successfully restore services in the event of an active database failure or crash. These activities are required to validate and strengthen the Business Continuity Plan (BCP).
23	Appendix 1B (S.No. 41)	5 (App 1B)	"The systems in cloud infrastructure should be updated with the latest anti malware signatures, the bidder shall submit the monthly report on the same with NABFINS."	Clarification on Anti-Malware Scope: As the core cloud-native SaaS platform is managed and secured natively by the OEM, please confirm that the requirement to update and report on anti-malware signatures applies only to local, bidder-managed collector VMs (log forwarders) deployed on-premises, and not the cloud-native SaaS backend	This point pertains to ensuring that the SIEM application hosting infrastructure and its associated components are adequately secured, with the latest anti-malware signatures updated. The Bidder/OEM shall provide confirmation of compliance with this requirement.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
24	Appendix 1B (S.No. 54)	6 (App 1B)	"Do not use Cryptographic Erase (CE) to purge media if the encryption was enabled after sensitive data was stored on the device..."	Request to Accept Cloud-Native Deletion: In a shared, distributed cloud-native storage architecture, physical media purging is controlled by the CSP using secure deletion policies (such as NIST SP 800-88). Please confirm that standard logical deletion and CSP-certified storage sanitization meet this compliance requirement.	Logical deletion alone shall not be considered sufficient for compliance where sensitive data has been stored prior to encryption. For cloud-native storage architectures where physical media sanitization is managed by the CSP, NABFINS may accept the CSP's secure storage sanitization/deletion processes, provided they comply with applicable regulatory requirements, Government of India advisories, or master directions. The Bidder/CSP shall provide appropriate certification, attestation, or audit evidence confirming secure deletion/sanitization and ensuring that the deleted data cannot be recovered or accessed.
25	Appendix 2 (Software License Page 4)	4 (App 2)	"Licensing Metrics: Please select the licensing metrics: As per NABFINS Projection Annexure 18"	Clarification on SaaS Licensing Metrics: Modern SaaS SIEMs (like Google SecOps) utilize simplified licensing models based on user/analyst seats or overall data volume (GB/day), rather than charging a fee per individual integrated source node (as listed in Annexure 18). Please confirm that bidders are permitted to propose their standard native licensing metrics (e.g., Platform/User License).	Please refer to the corrigendum.
26	Appendix 1A (SIEM_118)	4 (App 1A)	"Threat Hunting Query Support (KQL/SPL/SQL-like Query Capability) [Must Have]"	Clarification on Native Query Languages: While KQL/SPL are proprietary to specific legacy SIEM vendors, modern engines utilize equivalent, powerful native correlation languages (such as YARA-L). Please confirm that any platform-native query and correlation language which delivers equivalent threat hunting capabilities will be graded as "Standard" (10 marks).	Please refer to the corrigendum.
27	Main RFP (Sec 6.1, Clause m) VS Appendix 1A (SIEM_025)	Page 18 (RFP) & Page 2 (App 1A)	Main RFP: "Preferably, logs for 1–2 months shall remain online, after which they may be moved to archival storage." Appendix 1A (SIEM_025): "Minimum 365-Day Online Log Retention [Must Have]"	The main RFP specifies 1–2 months of online retention, while Appendix 1A requests 365 days. We are highlighting that Google SecOps provides 12 months of hot, searchable logs by default, as confirmed in Query No. 2's description, Please clarify.	Please refer to the corrigendum.
28				Request for extension The current bid submission timeline is 26-08-2026. Request you to kindly extend the bid submission timeline by atleast two (2) weeks from the date of publishing of corrigendum	Please refer to the corrigendum.
29	6.1 Cloud & CSP Requirements (f); Annexure 15 (Sizing Adequacy)	21, 96	"Bidder should arrive at the sizing independently. In case, the sizing quoted by the Bidder fails to meet the necessary services, NABFINS will not bear any cost."	Please share the sustained AND peak EPS (Events Per Second) of the current/expected environment. If EPS is not available, please provide the average and peak daily log volume (GB/day). This is the primary driver of SIEM licensing.	Please refer to the corrigendum.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
30	6.1 Scope of Core Services (SIEM Solution); Appendix 1B	19	"Log Parsing and Normalization … Validate log collection … Configure parsers and field mappings."	Is network flow monitoring (NetFlow/QFlow) in scope? If yes, please indicate the expected Flows Per Minute (FPM) / average network throughput.	Network flow monitoring (NetFlow/QFlow) is in scope where supported by the existing network infrastructure and required for security monitoring. The bidder shall support collection, parsing, normalization, and analysis of available flow records from the relevant network devices. The exact Flows Per Minute (FPM) and network throughput shall be assessed and finalized during the implementation/technical assessment based on the actual network environment. Bidders shall consider sufficient capacity to accommodate the existing traffic volume. Regarding EPS log volume, Please refer to the corrigendum.
31	6.1 Cloud & CSP Requirements (f, k, l); 8.22 Contract Period	21, 22, 52	"… during the contract period, growth of NABFINS should be considered … capacity planning can handle load and volumes till the end of contract period."	What is the anticipated year-on-year growth in EPS / log volume over the 3-year term (plus the 2-year extension), so that licensing and storage headroom can be correctly sized?	Please refer to the corrigendum.
32	6.1-B System Design (ix); Annexure 18 (Existing Infrastructure)	27, 28	Integration list: Network Devices, Windows/Linux/DB/Web Servers, AD/DNS/DHCP, Endpoint Security/EDR, IDS/IPS, DLP, Cloud Platforms, Virtualization, Third-party APIs, etc.	Please provide a consolidated asset inventory with device counts by category (Windows / Linux / DB / Web-App servers, firewalls, routers/switches, IPS-IDS, VPN/NAC, WAF, proxy, AD/DNS/DHCP, endpoints/EDR, DLP, cloud accounts, SaaS apps).	Details already given in the Annexure 18 (Existing Infrastructure). Additional details will disclosed with success ful bidder. Regarding EPS log volume, Please refer to the corrigendum.
33	6.1 Detailed Scope of Work (a); 6.1-B System Design (ix)	18, 27	"Configuration and Integrations at the NABFINS sites. Ensure that logs are being collected from all in-scope devices."	What is the total number of log sources to be onboarded at Go-Live, and the expected number of additional sources during the contract term?	Details already given in the Annexure 18 (Existing Infrastructure). Additional details will disclosed with success ful bidder. Regarding EPS log volume, Please refer to the corrigendum.
34	6.1-B System Design (ix) items 11, 12	28	"Endpoint Security/EDR, Antivirus Solutions … Windows Servers, Linux/Unix Servers, Database Servers, Web Servers."	Approximately how many endpoints (workstations + servers) are in scope, and is endpoint/EDR telemetry to be ingested into the SIEM, or is console integration only required?	Details are already provided in Annexure 18. Endpoint machines do not need to be individually integrated with the SIEM; only the centralized console is required to be integrated.
35	4.1 Overview; 6.1 Detailed Scope of Work (i) Helpdesk	9, 14	"… client base of nearly 11 lakh borrowers from 19 States …"; helpdesk support from NABFINS premise in Bangalore.	How many branches / field offices generate in-scope logs, and are branch-level device logs in scope, or only DC-hosted infrastructure & SaaS applications?	Details are already provided in Annexure 18 (Existing Infrastructure), covering the NABFINS Head Office infrastructure, centralized consoles, and SaaS infrastructure and services.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
36	6.1 (y) Production Environment	23	"DC - Primary Site (Standalone deployment) … Secondary Site (Standalone deployment) - To be made available throughout the contract period."	Please confirm whether the SIEM is required in Active-Active or Active-Passive mode across DC & DR, and whether DR is to run hot / warm / cold. This materially changes the license count and infrastructure cost.	It shall be the Bidder's responsibility to ensure real-time database synchronization and availability of the Disaster Recovery (DR) site. NABFINS will initiate the application switchover to the DR site as and when required.
37	6.1 Detailed Scope of Work; 6.1-F Resource Requirement	18, 30	"… 24*7 monitoring of NABFIN's Infrastructure … Availability of L1 & L2 resource 24*7*365 Support."	Is the scope SIEM platform management only, or full 24x7 SOC monitoring & incident response (MDR)? If SOC monitoring is in scope, please confirm the L1/L2 shift model and whether L1 monitoring is remote (bidder SOC) or onsite.	The support requirement is limited to SIEM tool-related issues, technical support, and configuration support and does not include SOC monitoring. NABFINS requires one dedicated engineer to be deployed at NABFINS Head Office during working hours to provide SIEM and incident management support.
38	6.1-F Resource Requirement (Resource table)	30, 31	"L2 Support Engineer (SOC Engineer) – Onsite Full time … 100% Dedicated Resource for NABFINS."	Please confirm the number of NAMED onsite L2 SOC engineers required, and whether onsite coverage is 24x7 or business-hours onsite plus remote after-hours.	One resource shall be deployed onsite at NABFINS during business hours. The roles and responsibilities of the resource are already defined in the RFP.
39	6.1 Scope of Core Services (item 5)	19	"Alerting and Incident Integration … Integrate with ITSM/SOAR platforms (e.g., In house Ticket, Jira, zoho ticket tool)."	Is a dedicated SOAR platform required as a separately licensed module, or is the SIEM's built-in workflow automation sufficient?	This particular point not asking for dedicated SOAR platform, provided the SIEM's native workflow automation/orchestration capabilities meet the required alert enrichment, automated response/workflow, escalation, and ITSM integration requirements. Integration with Jira and Zoho Ticket/Helpdesk shall be supported through standard APIs/connectors.
40	6.1 Scope of Core Services; Appendix 1B	19	"Use Case Implementation … Develop custom detection rules and correlation logic … Configure MITRE ATT&CK mapping."	Is UEBA (User & Entity Behaviour Analytics) or is core SIEM (log collection + correlation) sufficient?	The SIEM shall support custom detection rules, correlation logic, threat detection and MITRE ATT&CK mapping. Native UEBA capabilities may be considered as an additional/value-added feature.
41	4.2 Project Objective; 6.1 Responsibility Matrix	9, 24	"Bidder is required to Conduct transition of existing application, IT Infrastructure & services from existing vendor and perform data migration activities."	Is there an existing / incumbent SIEM? If yes, which product, and is historical log data migration in scope — if so, what data volume (GB/TB) and how many months of history?	Please refer to the corrigendum.
42	6.1 Scope of Core Services (item 5); 6.1 Detailed Scope (i)	14, 19	"Integrate the event with NABFINS's ticketing tool … (e.g., In house Ticket, Jira, zoho ticket tool)."	Which ITSM/ticketing tool will be integrated (in-house / Jira / Zoho), and is that ITSM license provided by NABFINS or to be included by the bidder?	This RFP is for the SIEM tool, with requirements limited to ITSM/Ticketing tool integration. Currently, NABFINS uses Zoho Helpdesk and Jira as its ticketing tools.
43	6.1-B System Design (ix) items 1, 6, 7	27	"Core MFI Solution … SaaS Application Logs … SaaS Application hosted Infrastructure."	For custom / legacy applications (e.g., Core MFI) requiring bespoke parsers, will NABFINS provide log samples and API access during implementation? Please list any non-standard log sources.	Yes. Details will be discussed with the successful bidder.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
44	6.1 Detailed Scope of Work (m); 6.1 (y) viii	16, 18	"Bidder shall store all logs for a minimum period of one year. Preferably, logs for 1–2 months shall remain online, after which they may be moved to archival storage."	Please confirm total log retention (RFP states minimum 1 year, 1–2 months online). Is any longer retention required for specific RBI/regulatory logs, and is archival storage to be priced within the same BoM?	Please refer to the corrigendum.
45	Section 5 - Eligibility Criteria, Note (repeated verbatim in Annexure 10)	13 and 102	"Either the bidder on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the said RFP. In a situation where multiple bids from the same solution (OEM Make) are received, all the bids of the same OEM product shall be liable for rejection."	Could NABFINS kindly clarify whether a bidder holding a valid OEM-signed MAF would remain eligible if an unrelated bidder independently proposes the same OEM product?	Yes.
46	Section 6.1 Training; Appendix 2 Instructions Tab V	41-42; Appendix 2	Section 6.1 Training: "Bidder will be required to provide Technical, Functional, Operational, User and system level training to NABFINS staff at NABFINS premises in-person / through WebEx/MS Teams" / Appendix 2 Tab V: "Bidder is required to factor in the required cost as a part of the implementation cost"	How many NABFINS personnel are to be trained, in how many batches, and at which locations?	5 Technical engineers at NABFINS Head office,Bangalore.
47	Section 4.2 – Project Objective	10	Bidder is required to design, size, supply, implement and deploy adequately sized and scalable hardware, software and cloud infrastructure.	What is the current average EPS (Events Per Second) and Peak EPS expected for the SIEM platform? This information is required for accurate SIEM sizing and licensing.	Please refer to the corrigendum.
48	Section 4.2 – Project Objective	10	Bidder is required to design and size the complete cloud solution.	What is the expected log ingestion volume (GB/TB per day)? This is required to size storage, compute and licensing accurately.	Please refer to the corrigendum.
49	Section 6.1(a) – SIEM Configuration & Integration	18	Ensure that logs are being collected from all in-scope devices and integrated with SIEM.	How many total log sources are to be integrated during Phase-1 and Phase-2? Please provide the approximate count by device/application category.	Details are already provided in Annexure 18 (Existing Infrastructure), covering the NABFINS Head Office infrastructure, centralized consoles, and SaaS infrastructure and services. The implementation phases will be discussed and finalized with the successful bidder.
50	Section 4.2 – Project Objective	9–10	Bidder shall implement SIEM across identified infrastructure, applications and IT assets.	Can NABFINS share the detailed inventory of servers, endpoints, firewalls, network devices, databases, applications and SaaS platforms that are in scope for SIEM integration?	Details are already provided in Annexure 18 (Existing Infrastructure), covering the NABFINS Head Office infrastructure, centralized consoles, and SaaS infrastructure and services.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
51	Section 4.2 – Project Objective	9	SIEM to be implemented across NABFINS infrastructure hosted on cloud and IT assets across India.	How many branches, regional offices, DCs, DR sites and cloud environments are part of the project scope? Please provide the deployment locations.	Details are already provided in Annexure 18 (Existing Infrastructure), covering the NABFINS Head Office infrastructure, centralized consoles, and SaaS infrastructure and services.
52	Section 6.1(m) – Log Storage & Retention	18	Logs shall be stored for a minimum period of one year with online and archival storage.	Beyond the mandatory one-year retention, what are the Hot, Warm and Archive storage requirements? Please specify expected retention duration for each storage tier.	Please refer to the corrigendum.
53	Section 6 – Core Services (Alerting & Incident Integration)	19	Integrate with ITSM/SOAR platforms (e.g., In-house Ticket, Jira, Zoho Ticket Tool).	Is SOAR part of this procurement or is only integration with an existing SOAR platform required? If existing, kindly specify the platform details.	This particular point not asking for dedicated SOAR platform, provided the SIEM's native workflow automation/orchestration capabilities meet the required alert enrichment, automated response/workflow, escalation, and ITSM integration requirements. Integration with Jira and Zoho Ticket/Helpdesk shall be supported through standard APIs/connectors.
54	Section 6(o) – Support Requirements	15	Availability of L1 and L2 resources on 24×7×365 basis.	How many SOC resources (L1/L2/L3) are expected onsite and offshore for steady-state operations? Please share the expected deployment model.	NABFINS requires one dedicated L3 resource for SOC and technical support. All other resources shall support SIEM solution implementation, configuration, and integration activities. The dedicated L3 resource shall be available onsite at the NABFINS Head Office, Bengaluru, during the required support hours.
55	Not Mentioned in RFP	—	Connectivity model between NABFINS and Bidder SOC is not specified.	Will NABFINS provide MPLS, VPN, ExpressRoute, Direct Connect or any dedicated connectivity to the Cloud SOC, or should the bidder provision the connectivity as part of the solution?	NABFINS will provide the necessary network access/connectivity from its premises to enable secure integration with the Bidder's Cloud SOC. The Bidder shall propose and provision the required secure connectivity mechanism as part of the solution, based on the proposed architecture and security requirements. The connectivity may be established through site-to-site VPN, dedicated connectivity, or other secure industry-standard mechanisms, subject to NABFINS's approval. The Bidder shall clearly specify the connectivity architecture, bandwidth requirements, and security controls. All associated expenses and costs shall be included in the Commercial Bid. No additional payment shall be made by NABFINS towards SIEM implementation, maintenance, support, or related services beyond the quoted commercial bid.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
56	Section 6(s) – DC & DR Support	15	Bidder shall maintain the solution at both DC and DR sites of the CSP.	What are the required Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the SIEM platform and associated cloud infrastructure to design the appropriate DR architecture?	The Bidder shall ensure that standard RTO and RPO practices are implemented and aligned with all applicable regulatory requirements and security standards. The RTO and RPO requirements specified in the RFP shall be strictly adhered to.
57	5. Eligibility Criteria-clause no. 10	11 to 12	ISO 27017	Request for Relaxation: We request NABFINS to relax the requirement of mandatory ISO 27017 certification. ISO 27017 is primarily applicable to Cloud Service Providers (CSPs) offering cloud infrastructure services, whereas the OEM in this RFP is providing the SIEM software platform. Since the proposed cloud infrastructure is to be hosted on a compliant CSP meeting the required certifications, we request that this requirement be made optional for the OEM or considered fulfilled through the proposed CSP.	ISO 27017 certification is mandatory for Cloud Service Providers (CSP) hosting the application and database. For the bidder/OEM, this certification is optional.
58	5. Eligibility Criteria-clause no. 10	11 to 12	ISO 27018	Request for Relaxation: We request NABFINS to relax the requirement of mandatory ISO 27018 certification for the OEM. ISO 27018 is intended for protection of Personally Identifiable Information (PII) in public cloud environments and is generally applicable to Cloud Service Providers. As the SIEM OEM is not acting as the cloud hosting provider, we request that compliance through the proposed CSP be accepted or that this certification be made optional for the OEM.	ISO 27018 certification is mandatory for Cloud Service Providers (CSP) hosting the application and database. For the bidder/OEM, this certification is optional.
59	5. Eligibility Criteria-clause no. 4	10 to 11	Average turnover ₹300 Crore (last 3 FY)	Request for MSME Relaxation: We request NABFINS to kindly provide an exemption from the OEM average annual turnover criterion of ₹300 Crore for OEMs registered as MSME/Udyam. The proposed SIEM solution is a specialized cybersecurity product, and the technical capability, product maturity, successful deployments, and compliance with the functional requirements are more relevant than the turnover of the OEM. Granting this relaxation to MSME OEMs will encourage participation of innovative Indian cybersecurity companies, promote fair competition, and support the Government of India's MSME, Make in India, and Atmanirbhar Bharat initiatives without compromising the quality of the solution. Therefore, we request that MSME/Udyam-registered OEMs be exempted from the ₹300 Crore average annual turnover requirement, subject to meeting all other technical and functional eligibility criteria.	No change in RFP.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
60	General	NA	Sizing Information Request	The RFP does not specify the expected number of log sources, average/peak EPS (Events Per Second), daily log ingestion volume, retention sizing, or the number of endpoints, servers, network devices, and applications to be integrated. Since these parameters are essential for accurately sizing the SIEM licenses, cloud infrastructure, storage, and commercial proposal, we request NABFINS to kindly provide: Total number of log sources Average EPS and Peak EPS Average daily log volume (GB/TB per day) Number of Windows/Linux servers Number of endpoints Number of network/security devices Number of cloud workloads and SaaS applications Required online and archive log retention capacity This information will enable bidders to size the solution accurately and submit a competitive and technically compliant proposal.	Please refer to the corrigendum.
61	eligibility criteria under Point No. 11			we have completed a SIEM project for a well-known BFSI customer outside India. The project involved implementation of SIEM capabilities in a BFSI environment and demonstrates our relevant technical expertise and experience in this domain. In view of the above, we kindly request you to consider providing suitable relaxation in the eligibility criteria under Point No. 11, thereby enabling us to participate in this RFP.	No change in RFP.
62	General Scope		Could you please provide an estimated daily data ingestion volume (e.g., in GB/day) and the expected Events Per Second (EPS)?	This is fundamental for accurately sizing the SIEM solution, determining the necessary infrastructure, and providing a precise cost estimate.	Please refer to the corrigendum.
63	5. Eligibility Criteria, Point 3		Can you please provide more clarification on the definition of an "IT Application & Maintenance company"?	As a product-based company, Exabeam's primary focus is on software development and not on IT application maintenance in the traditional sense. This query will help clarify if Exabeam, as a SIEM product company (OEM), is eligible.	Yes. As a SIEM product company (OEM), the organization is engaged in SIEM software development, product maintenance, upgrades, and technical support. Accordingly, we have requested the Certificate of Incorporation to verify that the OEM is a Software Development, IT Application & Maintenance company, registered/incorporated under the Indian Companies Act, with at least 10 years of existence in India as of the bid submission date.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
64	6.1 Detailed Scope of Work		Does the scope include the development of custom dashboards, correlation rules, and reports based on NABFINS's specific use cases?	This will help in scoping the professional services effort required for the initial implementation and tailoring the solution to your specific security monitoring needs.	Yes, please refer to the "Scope of Core Services" on Page 19 of the RFP for further clarity. The requirement is primarily to maintain the existing standard dashboards, rules, and reports already in place. No significant or additional development is envisaged.
65	6.1 Detailed Scope of Work, Point k		Please clarify the specific RBI regulations and laws of the land that the SOC needs to be compliant with.	While Exabeam is compliant with major global and Indian regulations, a specific list will ensure that all requirements are met.	As NABFINS is regulated by the RBI, the proposed solution and its infrastructure shall comply with all applicable RBI regulations and guidelines. Please refer to Clause 8.34 – "Adherence to Laws and Standards" on Page 57 of the RFP. Any future regulatory guidance or requirements issued by the RBI or other applicable regulators shall also be adhered to.
66	6.1 Detailed Scope of Work, Point m		Can you please specify the format and method for downloading the logs?	This will help in understanding the technical requirements for log retrieval and storage.	Please Refer to the corrigendum.
67	6.1 Detailed Scope of Work		Could you please define the expected performance difference between "online" and "archival" storage? For instance, are "online" searches expected to be interactive (seconds/minutes) while "archival" searches can take longer (hours)?	This will help set clear expectations. Exabeam can search across all data, but performance varies between hot and cold tiers. Defining this helps manage expectations around the "one day's notice" SLA.	Yes. Online searches are expected to be interactive, with visibility through the dashboard. Archival refers to data being stored for retention purposes. In case of a detailed investigation or specific requirement, NABFINS may request archived data, which the vendor shall provide within a one-day SLA.
68	6.1 Detailed Scope of Work		Can you provide an estimate of the frequency and volume of log retrieval requests you anticipate from archival storage? For example, do you expect this to be a weekly, monthly, or quarterly activity, and for what volume of data?	The "no additional cost" requirement makes this critical. Frequent or large-scale data retrieval from archival storage incurs significant cloud costs. An estimate is needed to price this risk into the bid.	Please refer to the corrigendum.
69	6.1 Detailed Scope of Work		In what format do you expect the logs to be "downloaded"? For example, is a CSV/JSON export from the SIEM interface sufficient, or is there a requirement for a specific raw log format delivered via another mechanism?	This clarifies the technical requirement for the export feature and ensures our standard capabilities meet the need.	Please refer to the corrigendum.

Response to Pre-Bid Queries (Tender Ref No: NABFINS/RFP/004/2026-27)					
Query No	**RFP Section (point number)**	**Page no.**	**RFP Excerpt**	**Query Description/Clarification sought**	**NABFINS Response**
70	6.1 Detailed Scope of Work		Regarding the "no additional cost" for log retrieval, does this apply to an unlimited number of requests? Would you be open to a model where a certain number of archival searches/retrievals per quarter are included, with a defined rate for additional requests?	This directly addresses the commercial risk and proposes a fair, transparent model that is common for cloud services. It protects both parties from unpredictable costs.	No change in RFP.
71	8.22 Contract Period		Is the 2-year extension of the contract subject to a competitive re-bidding process?	This will provide clarity on the long-term engagement and business opportunity.	Please refer to the RFP.
72	10.7 Technical Bid Evaluation Criteria		The Bidder should have office/ service/support centre with active operations located in Bengaluru. Undertaking from Bidder	Could you please clarify if the requirement for an office in Bengaluru applies to the bidding partner, the OEM, or both?	This clause is applicable only to the Bidder.