SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

Annexure-2 for RFP Ref: KaGB/Project Office/RFP/03/2021-22 dated 07.02.2022

Selection of Security System Integrator to Setup Cyber Security Operation Centre in Karnataka Gramin Bank & Kerala Gramin Bank

SIEM:

Sl. No	Requirement	Essential (E) or Preferable (P)	Compliance (Yes/No)	Remarks (Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
1	The proposed solution should be an appliance or Software with a clear physical or logical separation of the collection module, logging module and co-relation module.	E		
2	The proposed solution licensing should be by the number of events per second.	E		
3	The proposed solution should support log collection, correlation and alerts for the number of devices /applications mentioned in scope of work.	E		
4	The proposed solution should be able to support automatic updates of configuration information with minimal user intervention. i.e. security updates, vendor rule updates, device integration support, etc.	P		
5	The proposed solution must ensure all the system components continue to operate when any other part of the system fails or loses connectivity.	E		
6	The proposed solution must have an automated backup/recovery process.	E		
7	The proposed solution must automate internal health checks and notify the user in case of problems.	P		

8	The proposed solution should be able to perform single device & multi-device correlation across the network.	E		
9	The proposed solution should provide collection of events through customization of connectors or similar integration for the assets that are not natively supported. They should adhere to industry standards for event collection but not limited to the following syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, XML file.	E		
10	The proposed solutions should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.	E		
11	The proposed solution should have connectors to support the listed devices/ applications, wherever required the vendor should develop customized connectors at no extra cost	E		
12	In the proposed solution, all logs should be Authenticated (time-stamped across multiple time zones) encrypted and compressed while storing.	E		
13	The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service	E		
14	The proposed solution should provide options to load balance incoming logs to multiple collector instances.	P		
15	The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, AIX,Unix, Linux, Solaris servers etc.	E		
16	The proposed solution should be able to store/retain both the log meta data and the original raw message of the event log for forensic purposes.	E		

17	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	E		
18	The proposed solution shall allow bandwidth management, rate limiting, at the log collector level.	P		
19	The proposed solution should ensure that the overall load on the network bandwidth at DC/DR, WAN level is minimal	P		
20	The proposed solution should provide time based, criticality-based store and forward feature at each log collection point	E		
21	The proposed solution should have the capability to compress the logs by at least 70 % for storage optimization.	E		
22	The proposed solution should be possible to store the event data in its original format in the central log storage	P		
23	The data archival should be configured to store information in tamper proof format and should comply with all the relevant regulations.	E		
24	Traceability of logs shall be maintained from the date of generation to the date of purging.	E		
25	The proposed solution must support log archives on 3rd party storage.	E		
26	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	E		
27	The proposed solution should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.	E		
28	The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	E		

29	The proposed solution should provide mechanism that guarantee delivery of events to the log management system and that no events will get lost if log management system is unavailable	E		
30	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.	E		
31	The proposed solution should allow the creation of an unlimited number of new correlation rules	E		
32	The proposed solution should be able to integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating events. These data feeds should be updated automatically by the proposed solution.	E		
33	The proposed solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based etc., across potentially disparate devices.	E		
34	The proposed system/solution should have the ability to correlate all the fields in a log	E		
35	The proposed solution should be able to parse and correlate multi line logs	P		
36	The proposed solution should have the ability to gather information on real time threats and zero day attacks issued by anti-virus or IDS/ IPS vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds	E		
37	The proposed solution should allow a wizard-based interface for rule creation. The proposed solution should support logical operations and nested rules for creation of complex rules	E		

38	The central correlation engine database should be updated with real time security intelligence updates from OEM	E		
39	The dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	E		
40	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	E		
41	The dashboard should show the status of all the tools deployed as part of the SIEM, including availability, bandwidth consumed, system resources consumed (including database usage)	P		
42	It should be possible to categorize events while archiving for example, events for network devices, antivirus, servers etc.	P		
43	Any failures of the event collection infrastructure must be detected, and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events	E		
44	The proposed solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports. In addition, the proposed solution should have a reporting writing tool for development of any ad-hoc reports.	E		
45	The Dashboard design for the proposed solution should be editable on an ad hoc basis as per the individual user need	P		
46	The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard	E		
47	The proposed solution should allow applying filters and sorting to query results.	E		

48	The proposed solution should allow creating and saving of ad hoc log queries on archived and retained logs. These queries should be able to use standard syntax such as wildcards and regular expressions.	E		
49	The proposed solution should provide event playback for forensic analysis.	P		
50	The proposed solution should allow for qualification of security events and incidents for reporting purpose. The proposed solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/ incidents.	E		
51	The proposed solution should provide summary of log stoppage alerts and automatic suppression of alerts.	E		
52	The proposed solution should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM	E		
53	The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents, permit upload of related evidences such as screenshots etc.	E		
54	The proposed solution should be able to provide asset details such as Asset owner, location, events & incidents, vulnerabilities and issue mitigation tracking mapped to individual assets/users	P		
55	The proposed solution should provide knowledge base and best practices for various security vulnerabilities	E		
56	Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details	P		
57	Dashboard should capture the security status of assets and highlight risk level for each asset. This should be used to capture security status of bank, status of different business units within the bank, status of key locations etc.	P		

58	Dashboard should support monitoring, alerting and reporting for consolidated relevant compliance across all major standards and regulatory requirements in real time. This includes (but not limited to): ISO 27001, RBI regulations, IT ACT, PCI DSS standards, and NABARD regulations.	E		
59	Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department	E		
60	Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats	E		
61	Dashboard views should be customizable as per user rights and access to individual components of the application.	E		
62	Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard.	E		
63	Senior Management should be able to view compliance to SLA for all SOC operations	E		
64	The proposed solution should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.	E		
65	The proposed solution should have the capability to identify frequently used queries and provide means to optimize query response time for such queries	E		
66	The proposed solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	P		
67	The proposed system should identify the originating system and user details while capturing event data.	E		
68	The proposed solution should be possible to automatically create incidents and track their closure	E		

69	The event should reach the SOC monitoring team within minimum no of seconds, of the log being captured	P		
70	Pre-defined parsers are available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	P		
71	The proposed solution should be able to conduct full packet capture and securely store these packets for a minimum of 30 days	E		
72	The proposed solution should be able to intercept and review the SSL/TLS encrypted packets.	E		
73	The SSL decryptor should be able to support the standard ciphers for TLS and SSL protocols like TLS 1.3, 1.2, 1.1. and 1.0. The list of CIPHERS to be supported are mentioned in Annexure-24. Supporting documents for the same has to be provided by the vendor. Provisions must be available to upgrade the SSL decryptor in case of any changes of the ciphers used by the Bank. SI should provide any updated ciphers provided by the OEM regularly and as and when available.	P		
74	The proposed solution should have a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.).	E		
75	The proposed solution must provide embedded workflow capabilities that security operations staff can use to guide their work.	P		
76	The proposed solution should have the ability to send notification of correlated events via well-defined methods (SMS, email, etc.)	E		
77	The proposed solution should offer a means of escalating alerts between various users of the proposed solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.	E		
78	The proposed solution should provide indexing of all data in packets to simplify navigation across data.	E		
79	The proposed solution should be able to perform full reconstruction of session / events.	P		

80	Support importing of PCAP files, other structured and unstructured content for analysis.	P		
81	The vendor should provide for adequate storage to meet the EPS and retention requirements of the bank. SI shall be responsible for upgrade of the storage to meet the bank's requirements as above at no additional cost. The SI should provide adequate justification for the storage size proposed as part of the response.	E		
82	The proposed solution should be able to store both normalized and RAW logs	E		
83	The platform should provide tiered storage for the online, archival, and backup and restoration of event log information.	E		
84	The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin	P		
85	The storage solution should have the capability to encrypt/hash the logs in storage	E		
86	The proposed system should have capacity to maintain the logs for 90 days on box and 1-year logs on Tier I storage and 5 year logs should be archived on Tier II storage	E		
87	The proposed solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose automatically.	P		
88	The proposed solution should be able to filter logs before storage on the basis of type of logs; date etc.	P		
89	The proposed solution should be capable to replicate logs in Synchronous as well as Asynchronous mode.	E		
90	The proposed solution should be possible to define purging and retention rules for log storage.	E		
91	The proposed solution should come with built-in functionality for archiving data.	P		
92	The proposed solution should be able to receive database alerts from Database Activity Monitoring Tool (DAM)	E		

93	The proposed solution should be able to Integrate with IPS, IDS, Firewall, Proxy etc. to identify network security issues	E		
94	The proposed solution should be able to Integrate with DLP solutions to identify misuse of sensitive information	E		
95	The proposed solution should be able to integrate with in scope PIM and other Directory solution to relate security events to user activities	E		
96	The proposed solution should be able to integrate with in scope Vulnerability Assessment tools to identify security events	E		
97	The proposed solution should be able to integrate with GRC solution in future to capture compliance against security policies	E		
98	The proposed solution should be able to integrate with physical access control systems.	P		
99	The proposed solution should be able to Integrate with helpdesk/ ticketing tools	E		
100	The proposed solution Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	P		
101	The proposed solution should be able to integrate security logs with in scope existing Bank’s Applications.	P		
102	The proposed solution should ensure that all the logs are replicated and in sync in both DC and DR. The proposed solution should ensure that there should be no data loss.	E		
103	Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications	E		
104	The proposed solution should provide bi-directional integration with 3rd party trouble ticketing/help desk systems that security operations staff of the bank may use.	p		

105	The proposed system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.	E		
106	The SI should prepare a DR plan for switch over in case the DC operations are down	E		
107	The proposed solution should have high availability feature built in. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	E		
108	The proposed storage solution should have adequate redundancy for handling disk failures	E		
109	The proposed solution should be scalable as per bank roadmap for expansion	E		
110	The proposed Solution should support integration with big data storage configuration such as Hadoop etc.	P		
111	The proposed system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe.	P		
112	The Vendor must provide comprehensive support offering, including Phone Support, Email Support, Online community portal to access patches, upgrades new devices support and via online download	E		
113	The proposed solution should be preferably appliance-based solution	P		
114	The proposed solution should be capable of STIX and TAXII bi directionally and should be capable to integrate and auto configure Bank’s applicable devices at no cost to the Bank	P		

SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

Privileged Identity Management Solution (PIM)

Sl. No	Requirement	Essential (E) or Preferable (P)	Compliance (Yes/No)	Remarks (Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
1	The proposed solution Should control commands the privileged user is authorized to perform	E		
2	The proposed solution should provide the feature of keystroke logging for privileged users	E		
3	The proposed solution should support multi factor authentication for privileged users	E		
4	The proposed solution should be able to conduct session log capture for privileged users	E		
5	The proposed solution should be able to conduct session video recording for privileged users	E		
6	The video recorded should be of minimal size and the recording should not impact user work and system performance	E		
7	The proposed solution should be able to provide time-based sessions for privilege users	E		
8	The proposed solution support delegation by identity administrator to another person for a specific period of time	E		
9	The proposed solution support for reminders to identity administrators who are required to perform workflow tasks	E		
10	The proposed solution should support denial of access protection by blocking repeated password failures on multiple administrator accounts in the directory.	E		
11	The proposed solution should be able to delegate privileged access to commands or applications.	E		

12	The proposed solution should enforce segregation of duties as defined by the Bank.	E		
13	The proposed solution should provide audit information on where privileged accounts are enabled, which users have access to these and if this access is as per Bank policies including password requirements.	E		
14	The proposed solution should include an encrypted vault for privileged user credentials.	E		
15	The proposed solution should ensure tamper proof storage of password, credentials, recordings, and logs.	E		
16	The proposed solution should be able to develop privileged identity management audit reports (but not limited to): PCI DSS, RBI guidelines, NABARD regulations , Cert-In, NCIIPC and others.	E		
17	The proposed solution should include a software development kit to facilitate integration with home-grown/ in-house applications	E		
18	The proposed solution should be able to integrate with existing AAA authentication devices, directory services etc.	E		
19	The proposed solution should support for database-maintained change log for event triggered updates	E		
20	The proposed solution should have template-based workflows for user account creation, management, group assignments, de-activation and deletion	P		
21	The proposed solution support for event-driven and request driven account de-activation (i.e., not deletion)	P		
22	The proposed solution should support both workflow for disabling and deletion of accounts in separate steps as per Bank's requirements.	P		
23	The proposed System should have a web-based GUI for designing workflows	E		
24	The proposed solution should have a set of out-of-the-box reports to satisfy compliance requirements which should include:(But not limited)	E		
	· User logins and account details.	E		
	· Periodicity of access to specific accounts	E		

	· Periodicity of changes to user details including passwords	E		
25	The proposed system should support scheduled report generation	E		
26	The proposed system should support integration with external GRC, SIEM and HRMS	E		
27	Provide a built-in query tool for ad-hoc reporting	P		
28	The proposed solution should support for password push to selectable target systems (i.e., the user or administrator is allowed to specify which systems have the same password	P		
29	The proposed solution should control the following: Systems the user can access, methods of access such as local, remote, SSH, Telnet etc., sources of access such as workstation, IP address, VPN etc.	E		
30	The proposed solution should be able to authenticate users on the basis of the following (multiple factors for authentication): Username and password, Digital certificates, One-time passwords, Biometrics (such as fingerprints, iris scans etc.), Smart cards and tokens etc.	E		
31	The proposed solution should support for bulk password updates or resets based upon administrator-defined groups of users	p		
32	The proposed system should imbibe password controls as per Bank's requirements.	E		
33	The proposed system should support user maintenance auditing (identity updates, password changes, self-administration, etc.)	E		
34	The following events should be registered for audit purposes (but not limited to):	E		
	· Authentication events	E		
	· Authorization events	E		
	· Directory object modification	E		
35	Audit dashboard should list issues such as unauthorized access provisioning, list of users deactivated post due date etc.	E		
36	The proposed system should have a password check-in and check-out feature for privileged users. This should be based on appropriate workflows.	P		

37	The proposed system should enforce automatic change in password on first time sign in to prevent the admin to reuse the same password again.	E		
38	The proposed system should have the ability to control periodic password changes.	E		
39	The proposed system should be able to control the number of users who can access common/shared privileged IDs at any point of time.	P		
40	If the privileged users attempt to block session recordings, system should have the ability to raise appropriate alerts.	P		
41	The proposed solution should be able to automatically change privileged passwords for critical applications/ databases on a periodic basis. The system should then be able to provide access to applications that require to connect to these critical systems.	E		
42	The proposed solution should not act as a single point of failure for privilege access to systems and it should be possible to recover passwords during outages.	E		
43	The proposed solution should be able to integrate with vulnerability management solution to ensure that automated VA scans utilize privileged accounts for devices which are managed by the PIM solution	P		
44	The proposed solution should manage privilege accounts on virtual machines and should also enforce policies on newly detected virtual machines	P		
45	The proposed solution should provision, deprovision passwords to users and user groups in bulk.	E		
46	The proposed solution should capture every privileged session activity through audit trails for forensic investigations.	E		
47	The proposed solution should monitor privileged sessions and record every privileged user session with playback capabilities for post session review.	E		
48	The proposed solution should automatically lock down privileged accounts that are inactive for a period of time.	E		

49	The proposed solution should assign time-bound access to resources using start and end dates	E		
50	The proposed solution should provide notifications when privileged roles are activated	E		
51	The proposed solution should support password vaulting.	E		
52	The proposed solution should provide default dashboards or reports indicating below (not limited to the following) - - Orphaned accounts that could provide an attacker with a backdoor to the bank's critical infrastructure -Passwords with no expiration date -Inappropriate use of privileged passwords—such as using the same Admin account across multiple service accounts -SSH keys reused across multiple servers	P		
53	The proposed solution should implement one-time passwords (OTPs), which immediately expire after a single use for sensitive privileged access and accounts.	E		
54	The proposed solution should be capable of providing just-in-time privileges (JIT) privileges.	E		

SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

Anti – APT

S.No	Requirement	Essential (E) or Preferable (P)	Compliance (Yes/No)	Remarks(Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
1	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the Bank's network.	E		
2	The solution should be able to protect against Advanced Malware, web exploits and targeted threats without relying on signature database.	E		
3	The solution should be able to identify and prevent malware present in file types and web objects such as (QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll,ico, jar, jpeg, jpg, mov, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc.) and be able to quarantine them.	E		
4	The solution should be able to block malware downloads over different protocols.	E		
5	The solution should support on premise Sandbox test environment which can analyze threats to various operating systems, browsers, desktop applications and plug-ins etc.	E		
6	The solution should support both inline and out of the band mode.	E		
7	The solution should be able to detect and prevent bot outbreaks (via multiple channels like SMTP, HTTP, HTTPS etc.) including identification of infected machines	E		
8	The solution should be appliance based with hardened OS. No information should be sent to third party system for analysis of malware automatically. It is expected that the solution will send only hash values to anti-virus vendors to get signatures if the signatures are not available. It is expected that all analysis of malware will happen onsite in sandbox environment.	P		

9	The solution should be able to block the call back tunnel including fast flux connections.	E		
10	The solution should be able to integrate with deployed appliances to share malware information/ zero-day attacks knowledge base.	E		
11	The solution should be able to pinpoint the origin of attack both inside the network (infected machine inside the bank network) and outside the network (attempted attach from a remote C&C server) and should be able to block the communication with the affected machine/server.	P		
12	In case there is no antivirus signature available for malware, solution should have the ability to exfiltrate data about the malware and share it with the bank's existing antivirus solution providers. (The hash values maybe shared with the AV providers. The AV provider may be the proposed Anti-APT's own AV provider.	E		
13	The solution should be able to conduct forensic analysis on historical data.	P		
14	Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, attacked ports, source hosts etc.	E		
15	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.	E		
16	The solution should be able to export event data to Bank's existing SIEM or Incident Management Systems	E		
17	Solution should be able to monitor encrypted traffic	E		
18	The management console should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.	E		
19	The solution should display the geo-location of the remote command and control server.	P		
20	The solution should be able to integrate with the Active Directory / ICAP to enforce user-based policies.	P		
21	The solution should be capable of detecting and preventing the threats in real-time using sandbox evasion techniques such as Stalling Delays, User Action Required, Suspended Activities, ROP Evasion, Rootkits etc.	P		

SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

Vulnerability Management & Scanner

Sl. No	Requirement	Essential (E) or Preferable (P)	Compliance (Yes/No)	Remarks (Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
1	The proposed solution should have minimal impact on traffic, server performance, networks etc. during deployment and operation	E		
2	The proposed solution should maintain an updated database for latest vulnerabilities	E		
3	The proposed solution should provide flexible deployment of VAS solution and capability for tuning the scanning configurations for optimal performance of Bank's infrastructure	P		
4	The proposed solution should provide pre-built integrations with other security solutions	P		
5	The proposed solution should perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).	E		
6	The proposed solution should support application scanning, endpoints (laptops or desktops) scanning	E		
7	The proposed solution should support centralized management of scan operations, reporting and administration.	E		
8	The proposed solution should automatically discover and categorize assets based on multiple attributes and not just the IP addresses	E		
9	The proposed solution should be able to identify applications running on non-standard ports.	E		
10	The proposed solution should track hosts over time in a dynamic IP environment (DHCP)	P		
11	The vulnerability signature database should include breakdown of types of signatures (i.e. CGI, RPC, etc.) and number of signatures that map directly to CVE IDs.	E		
12	The proposed solution should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to: Windows, AIX, Unix, Linux, Solaris servers etc.	E		

13	The proposed solution should provide mechanism to upload IP lists of devices through XLS format	E		
14	The proposed solution should provide configurable Vulnerability assessment policy and individual tests	E		
15	The proposed solution should be able to scan workstation, servers, network and security equipment.	E		
16	The proposed solution should be able to run scans on network segments as well as entire network.	E		
17	The proposed solution should be able to perform authenticated and unauthenticated scans and manage credentials centrally for authenticated scans.	E		
18	The proposed solution should be able to scan application databases for vulnerabilities	E		
19	The proposed solution should be able to detect weak password for databases and point out accounts with simple, weak and shared passwords.	E		
20	The proposed solution should be able to identify out-of-date software versions, applicable patches and system upgrades.	E		
21	The system should be able to identify configuration deviations/defects as per bank baselines or CIS or SCAP or OVAL baseline/ Standards /leading practices for the various devices in scope	P		
22	The proposed solution should include vulnerability rating methodology configurable to Bank's requirement	P		
23	The proposed solution should provide remediation information in the reports including links to patches etc.	E		
24	The proposed solution should produce a report listing all applications on a host or network, regardless of whether the application is vulnerable	E		
25	The proposed solution should generate report in line with PCI DSS, ISO 27001, NABARD Regulations, CERT-In or RBI Guidelines.	P		
26	The proposed solution should be able to support “scan windows”, scan scheduling, and automatic/manual pausing/stopping/restarting of scans.	E		
27	The proposed solution should support users to modify existing rules or create their own rules	E		

28	The proposed solution should include a library of potential vulnerabilities and rules which should cover SANS top 20. This library should be customizable by the administrator and changes to the same should be traceable.	E		
29	The proposed solution should produce reports in any of the following formats: XLS, PDF, CSV, XML etc.	E		
30	The proposed solution vendor should assist the bank in reducing the number of false positives identified by the solution	E		
31	The proposed solution should be able to prioritize vulnerabilities on the basis of severity levels defined by the Bank	P		
32	The proposed solution should be able to track the closure of all vulnerabilities identified and should include parameters such as responsible person, date of closure, action taken etc.	E		
33	The proposed solution should generate reports on trends in vulnerabilities on a particular asset.	E		
34	The proposed solution should be able to integrate with other security solutions (i.e. SIEM, Patch Management etc.)	E		
35	The proposed Solution should have an Application Programming Interface (API) to integrate with other systems	E		
36	The proposed solution should integrate with the existing/ proposed WAF solution	P		
37	The proposed solution should support integration with threat feeds, allowing vulnerabilities to be correlated against real-time threat information.	E		
38	The proposed solution should be able to detect both wireless and rogue devices	E		
39	The proposed solution should support all kind of standard platforms (not limited to) and versions like AIX, Solaris, Linux, MAC OS and Windows etc.	E		
40	The proposed solution should maintain history of scan and provide comparison between two scans and differential reports of the scans	E		
41	The proposed solution should support discoveries of vulnerabilities caused by absence of update for OS, Database, Application, etc.	E		
42	The proposed solution should support scanning of virtualization and terminal platforms like vSphere, Hyper-V, XenApp, etc.	E		
43	The proposed solution should provide both pre-configured and fully customizable report templates for various stakeholders across organization.	E		

44	The proposed solution should provide Built-in reports that include but not limited to audit, baseline comparison, executive summary, PCI, policy compliance, remediation planning, top remediation, SANS Top 20, vulnerability verification report etc.	E		
45	The proposed solution should allow bank to schedule the VA of selected assets for a pre-defined date and time. The proposed solution should also be able to schedule scans based on asset ratings and asset types.	E		
46	The bidder should assist in building of scan templates as per Bank's requirements such as types of applications to be scanned, protocols to be used, ports to be scanned etc.	E		
47	The proposed solution should integrate with asset management systems available in the network.	P		
48	The proposed solution should provide a consolidated overview of all the digital assets with actionable security ratings and risk scoring.	P		
49	The proposed solution should support customizable reports	E		
50	The proposed solution should provide auto-synchronization of asset data to the central Server.	P		
51	The proposed solution should provide and support Import/Export of the Asset data	E		
52	The proposed solution should list each vulnerability found, gauging its level of severity, and suggesting to the user how this problem could be fixed.	E		

SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

Other General Requirements

Sl. No	Requirement	Essential (E) or Preferable (P)	Compliance (Yes/No)	Remarks (Bidder's Offer). Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.
	Security			
1	All proposed solutions should be IPv6 compatible from Day 1. The bidder should assist the bank in migration to IPv6 as and when the bank decides to migrate to IPv6 for devices in scope.	E		
2	All solutions should support 256 bit or higher encryption for transfer of information	E		
3	All solutions should support User Authentication Mechanism such as Directory Services and AAA as deployed in the bank's environment. The systems should be able to align to the bank's authentication requirements including password policy.	E		
4	Any changes to the solutions deployed should be logged including changes to database such as Update, insert, delete, select etc. (DML), Schema/Object changes (DDL), Manipulation of accounts, roles and privileges (DCL), Query updates.	E		
5	The proposed solutions should maintain the audit trail for the management activities of individual users and administrators accessing and using the application	E		
6	The systems should have a mechanism for protection of unauthorized access on the Log Database by system administrator and should maintain an auditable chain of custody.	E		
7	Solutions should provide for Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) and provide access based on the least privilege criteria	E		
8	All devices should comply with FIPS-140-2 standard for cryptographic modules	E		
9	All solutions deployed in inline mode should have built in bypass (fail open) for inline mode.	E		
10	All appliances should have dual power supply to ensure redundancy	E		
11	All devices/appliances should be rack mountable and 1U/2U type	E		
12	All the proposed solutions should support external storage such as SAN storage	E		
13	The solutions should support virtual environments	E		

	Support			
14	The bidder shall ensure that all deployed devices shall have the latest patches/ security upgrades.	E		
15	The bidder shall develop the following processes in co-ordination with the Bank for the operation of the SOC (but not limited to) 1. Configuration and Change Management 2. Incident and Escalation management processes 3. Daily standard operating procedures 4. Training procedures and material 5. Reporting metrics and continuous improvement procedures 6. Data retention and disposal procedures 7. BCP and DR plan and procedures for SOC 8. Security Patch management procedure	E		
16	The bidder should ensure the SLAs are adhered to and should provide the bank with periodic reports of the performance against the defined SLAs	E		
17	The bidder should provide continuous threat updates from sources such as CERT, ISAC, NIST, RBI etc.	E		
18	The bidder should assist the bank in performing analysis and optimization of log collection process	E		
19	Technical Support should be available through OEM or the registered partners of OEM and as per defined SLAs	E		
20	The bidder should develop, update and maintain log baselines for all platforms at the Bank	E		
21	The bidder should maintain a knowledge base of alerts, incidents and mitigation steps	E		
22	Evidence for any security incident should be made available for legal and regulatory purposes	E		
23	The bidder should have a Comprehensive system documentation, user guides and online help for devices.	E		
24	The bidder should ensure that events occurring at any of the devices/ applications etc. are logged and displayed at the SIEM within 30 seconds of their occurrence.	E		
25	All solutions should be saleable as per Banks future requirements.	E		

SELECTION OF SECURITY SYSTEM INTEGRATOR TO SETUP CYBER SECURITY OPERATION CENTRE (C-SOC) IN KARNATAKA GRAMIN BANK AND KERALA GRAMIN BANK

	Bidder Resources			
26	All the resources provided for monitoring of the product & administration of the solution should be as per Annexure-6.	E		
27	In case of exigencies even during off business hours / Bank holidays, the resources may be required to be present onsite	E		
28	Personnel deployed in the Bank premises shall comply with the Bank's Information Security Requirements.	E		
29	The SOC should be supported by 3 shifts for 24/7 operations, and the resources should be able to support and analyze data received	E		

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection.

Signature with seal

Name:
Designation