भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

# INVITATION FOR EXPRESSION OF INTEREST (EOI) FOR IDENTIFYING FILE INTEGRITY MONITORING (FIM) AND CONFIGURATION AUDIT (CA) IN A SINGLE SOLUTION PLATFORM

EOI Reference No: NPCI/EOI/2024-25/IT/03 dated 19th August 2024

National Payments Corporation of India
Unit no. 202, 2nd floor,
Raheja Titanium, CTS No. 201,
Western Express Highway,
Goregaon East, Mumbai 400 063
Email- itprocurement@npci.org.in
Website: www.npci.org.in

## Section-1: Background

**Background:**

**File Integrity Monitoring (FIM):** FIM is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline. Changes to configurations, files and file attributes across the IT infrastructure are common but hidden within a large volume of daily changes can be the few that impact file or configuration integrity. Values monitored for unexpected changes to files or configuration items include:

a. Credentials
b. Privileges and Security Settings
c. Content
d. Core attributes and size
e. Hash values
f. Configuration values

**Configuration Audit (CA):** CA help organizations maintain a detailed record of their software, hardware, and documentation throughout their lifecycle. By adhering to industry standards and regulations, businesses can demonstrate their commitment to security and compliance. Configuration Audit reduces the risk of unauthorized changes, configuration drift, and system failures. It ensures that IT assets remain in their desired state, minimizing downtime and enhancing system availability. Configuration audits help ensure that configuration items (CIs) have been developed and completed following the defined documents and requirements. This process ensures that changes are properly managed and controlled. Having a well-documented configuration baseline allows organizations to troubleshoot issues more efficiently. Audits verify that the configured products meet functional characteristics and requirements.

File Integrity Monitoring (FIM) and Configuration Audit are critical components of cybersecurity. They help organizations detect unauthorized changes, ensure compliance, and maintain the security and integrity of their systems. NPCI is looking for a single platform on prem solution which can provide features of File Integrity Monitoring (FIM) & Configuration Audit.

## Section-2: Requirement

This Expression of Interest (EOI) is floated in order to identify **OEMs** who have such File Integrity Monitoring (FIM) and Configuration Audit (CA) in a single solution platform.

## Section-3: Technical Specifications

Refer **Annexure-I.**

## Section-4: Response Submission

**Interested OEMs** who are having the required solution may please contact the NPCI team members as provided in the schedule below with platform details and feature compliance **(as per Annexure-I)**.

| Sr.No. | Description | Detailed Information |
|---|---|---|
| 1. | Name | Invitation for Expression of Interest for identifying file integrity monitoring (FIM) And configuration audit (CA) in a single Solution Platform |
| 2. | EOI Reference Number | NPCI/EOI/2024-25/IT/03 |
| 3. | Date of release of EOI | 19th August 2024 |
| 4. | Last date and time of receiving queries from OEMs | 23rd August 2024 5:00 PM |
| 5. | Last date and time for EOI Response Submission | 27th August 2024 5:00 PM |
| 6. | Email correspondence details | OEMs to send the communication (queries, bid response) to below mentioned email id's<br>siddhesh.chalke@npci.org.in<br>darshana.salunkhe@npci.org.in<br>benny.joseph@npci.org.in |

## ANNEXURE - I
## TECHNICAL SPECIFICATIONS

| S.No. | Features / Descriptions | Compliance Good to have/Must have | Compliance (Yes / No) |
|---|---|---|---|
| 1 | **File Integrity Monitoring** | | |
| 1.1 | As per NPCI requirement, the proposed solution should be completely on premise. An on-premise solution where NPCI will have complete control over the data, including where it is stored, how it is managed, and who has access to it. | Must have | |
| 1.2 | The proposed solution should be capable of DC/DR Setup with Clustered Database - Can be deployed in a Disaster Recovery (DR) configuration in order to automatically fail over to a Secondary console in the event of Primary console failure. | Must have | |
| 1.3 | The Proposed solution should have Single Centralized Console for FIM and SCM | Must have | |
| 1.4 | The proposed solution should be able to automatically check for changes to | Must have | |
| | · file/directory contents. | Must have | |
| | · file/directory permissions. | Must have | |
| | · file/directory time/date stamps. | Must have | |
| | · file/directory names. | Must have | |
| 1.5 | The proposed solution should have ability to automatically check for additions/modifications/deletions to Windows registry keys. | Must have | |
| 1.6 | Incase of Hardware the proposed solution should support dual power input facility | Must have | |
| 1.7 | The proposed Solution should support multiple hashing algorithms (e.g. MD5, SHA). | Must have | |
| 1.8 | The proposed Solution should have ability to detect changes to server file systems. | Must have | |
| 1.9 | The proposed Solution should have ability to detect changes to network devices. | Must have | |
| 1.10 | The proposed Solution should have ability to archive new versions of configurations as changes are detected and baseline configurations evolve. | Must have | |
| 1.11 | The proposed Solution should have ability to detect changes as frequently as required – in real-time and/or through a scan-based approach. | Must have | |
| 1.12 | The proposed Solution should have Comprehensive Multi-Platform Support: | Must have | |
| | · Operating Systems: Windows, Linux, Unix, AIX, Solaris etc | Must have | |
| | · Network Devices: Any type | Must have | |
| | · LDAP/AD: | Must have | |
| | · Privileged group by watching adds/deletes | Must have | |
| | · Difference between global and local policies | Must have | |
| | · Changes to group policy options | Must have | |
| 1.13 | Change IQ: Capability to quickly compare two versions of a change with a before and after view to change variance. Change IQ provides context such as - | Must have | |
| | · What Change was made | Must have | |
| | · Who made the Change | Must have | |
| | · When was the Change made | Must have | |
| | · Captures original regular account users using “Sudo” or “Su” commands in Linux/Unix. | Must have | |
| 1.14 | The proposed solution should have ability to provide standard sets of defaults File Integrity Monitoring rules for each operating systems which helps comply with regulatory requirements such PCIDSS, CIS, ISO and SOX compliances. | Must have | |

| | | | |
|---|---|---|---|
| 1.15 | The proposed solution should have ability to automatically check for changes to file/directory : | Must have | |
| | · permissions. | Must have | |
| | · time/date stamps. | Must have | |
| | · names. | Must have | |
| | · ownership. | Must have | |
| | · Can automatically check additions/modifications/deletions to Windows registry keys | Must have | |
| | · file content changes using cyclic redundancy checking and/or digital signature checking. | Must have | |
| 1.16 | The Proposed Solution should have ability to generate a baseline of a server(s) so that integrity is based on a known-good state. | Must have | |
| 1.17 | The proposed solution should have ability to remotely distribute policy files via a console to one or more machines. | Must have | |
| 1.18 | Policy templates of the proposed solution are available from vendor. | Good to Have | |
| 1.19 | The Proposed Solution should have ability to specify severity level to individual files and/or directories. | Good to Have | |
| 1.20 | The proposed solution should support file directory recursion. | Must have | |
| 1.21 | The Proposed Solution should have ability to have monitoring (view-only) only consoles available for defined users. | Must have | |
| 1.22 | The Proposed solution should have ability to easily and quickly update multiple baselines at once, in cases where routine maintenance and/or changes cause integrity violations. | Must have | |
| 1.23 | The Proposed solution should have Ability to automatically update baseline. | Good to Have | |
| 1.24 | The Proposed solution should have a Management console that is cross platform (i.e. Windows and Unix). | Must have | |
| 1.25 | Management console can detect status of agents. | Must have | |
| 1.26 | Allows users to quickly compare two versions and quickly isolate changes or differences between versions. | Good to Have | |
| 1.27 | The proposed solution should provide immediate access to detailed change information. | Must have | |
| | Arrange and manage monitored components in a number of ways including by location, device type, and responsibility. | Must have | |
| | Provides authorized users the ability to establish one specific version as a trusted configuration for each system. | Must have | |
| | Provides standard sets of defaults and templates for each operating environment | Must have | |
| | Ability to compare an asset's configuration state against a pre-defined policy to determine whether the configuration is compliant. | Must have | |
| | Seamlessly integrates with file integrity monitoring data to immediately reassess upon detected changes (continuous compliance). | Must have | |
| | Vendor supplied policy templates. | Must have | |
| 1.28 | The proposed solution should support Center for Internet Security (CIS) benchmarks out-of-the-box. | Must have | |
| | Supports security standards (NIST, DISA, VMware and ISO 27001) out-of-the-box. | Must have | |
| | The Proposed solution should have Support regulatory requirements (PCI, SOX, FISMA, FDCC, NERC, and COBIT) out-of-the-box. | Must have | |
| | Provides out-of-the-box remediation guidance to help fix non-compliant configurations. | Must have | |
| | Should have ability to systematically waive policy tests to seamlessly integrate into compliance processes & requirements. | Must have | |
| 1.29 | Should have ability to run configuration assessment on existing data without requiring a rescan. | Must have | |
| 1.30 | The Proposed solution should have ability to use same scan data in multiple, different policy checks without requiring a rescan. | Must have | |
| 1.31 | Ability to report "policy scorecards" to summarize the compliance status of a device. | Must have | |
| 1.32 | Ability to ignore certain tests for certain periods of time (i.e. support for policy waivers). | Must have | |

| | | | |
|---|---|---|---|
| 1.33 | The Proposed solution should have ability to report on current policy waivers in effect and their expiration dates. | Must have | |
| 1.34 | The agents must be Tamper-proof, i.e Users should not be able to stop the service even with Admin rights. | Must have | |
| 1.35 | The Proposed solution should have Ability to detect changes to : | Must have | |
| | · System and configuration files | Must have | |
| | · Application and service files | Must have | |
| | · Security and log files | Must have | |
| | · Database files | Must have | |
| | · Home directories | Must have | |
| | · Encryption and certificates files | Must have | |
| | · Sensitive configuration files(api keys,secrets etc) | Must have | |
| | · Backup configuration files | Must have | |
| 1.36 | The Proposed solution should have ability to detect changes of event reconciliation with change ticketing systems (e.g. SNOW, HP OpenView, BMC Remedy, Peregrine, Tivoli) to correlate and match requested change tickets to actual changes. | Good to Have | |
| 2 | **Configuration Assessment** | | |
| 2.1 | The proposed solution should have ability to use the same scan data in multiple, different policy checks without requiring a rescan | Must have | |
| 2.2 | The proposed solution should have ability to Provide out-of-the-box remediation guidance to help fix non-compliant configurations | Must have | |
| 2.3 | The proposed solution should have ability to Enable compliance with security and regulatory requirements (e.g. CIS, PCI, ISO, SOX, FISMA, FDCC, FFIEC, NERC, HIPAA, JSOX, GLBA, etc.) | Must have | |
| 2.4 | The proposed solution should Support vendor supplied policy templates | Must have | |
| 2.5 | The proposed solution should have ability to easily modify standard policies to conform to unique organizational needs | Must have | |
| 2.6 | The proposed solution should have ability to report “policy scorecards” to summarize the compliance status of a device. | Must have | |
| 2.7 | The proposed solution should have ability to systematically enable waive policy tests to seamlessly integrate into compliance processes and requirements. | Must have | |
| 3 | **Reporting / Alerting** | | |
| 3.1 | The proposed Solution should support multiple levels of reporting. | Must have | |
| 3.2 | The proposed Solution should provide executive level summary reports/dashboards. | Must have | |
| 3.3 | The proposed Solution should support Reports to be sent via email. | Must have | |
| 3.4 | The Proposed solution should be able to integrate & forward alerts to SIEM solution. | Must have | |
| 3.5 | The proposed Solution should support local archive of reports | Good to Have | |
| 3.6 | Reports provided clearly denote severity levels of integrity violations. | Must have | |
| 3.7 | The proposed solution should supportReports can be filtered and searchable. | Must have | |
| 3.8 | Reports can be exported to other applications (CSV, xml or html format). | Must have | |
| 3.9 | The proposed solution should support Reports creation on demand. | Must have | |
| 3.10 | The proposed Solution should Alert users of when configurations change, what change was made and who made the change. | Must have | |
| 3.11 | The Proposed solution's have Alerts that can be based on complex combinations of events using sets of criteria (Boolean logic) | Good to Have | |
| 3.12 | The Proposed solution should enable searches of configuration histories and audit logs for specified content using a variety of search criteria and filters. | Must have | |
| 3.13 | The Proposed solution should allow searching to be predefined or saved for future use by all users. | Must have | |
| 3.14 | The proposed Solution should be able to identify all devices whose configurations differ from their designated baselines, or either contain or are missing specified configuration settings. | Must have | |
| 3.15 | The proposed Solution should support Audit logging that provides a change control record for all change activity by recording detected changes, added and deleted devices, modified user accounts, etc. | Must have | |

| | | | |
|---|---|---|---|
| 3.16 | The proposed Solution should provides a role-based & customizable user interface. | Good to Have | |
| 3.17 | The proposed Solution should Provide the ability to create custom home pages for various users and user roles | Must have | |