TERMS OF REFERENCE

FOR

FOR AUDIT OF SAP FILE LIFECYCLE MANAGEMENT

Architecting e-Government

Contents

1 Data Sheet

Sl. No	Item	Description
1.	Organization	National Institute for Smart Government
2.	Mode of submission of bid	Softcopy
3.	Officer to whom bid shall be addressed	Bharath Mohan – 9702004505 Bharath.mohan@nisg.org
4.	Contact Details	**Primary contact.** Bharath Mohan – 9702004505 Bharath.mohan@nisg.org **Secondary contact** Murali Bomireddy – 99890 95111 Email id: murali.b@nisg.org
5.	Last date and time for submission	21st March 2026

2 Purpose of the Terms of Reference (ToR)

National Institute for Smart Government (NISG), Hyderabad, hereinafter called the **"NISG"**, having agreed with one of its clients, hereinafter called "**Client**" for providing Audit services of SAP FLM Module, is seeking proposals from prospective and qualified agencies /individuals, hereinafter called "**Service Provider**", who can provide technical expertise as per requirement/ services requested in this ToR.

The Service Provider can source prospective resources from multiple agencies. However, payments for engaging the resources shall be made only to the Service Provider / individuals with whom NISG enters into an agreement. The Service Provider shall be responsible for the performance of the services rendered.

3 Scope of Work & Deliverable

NISG's client is based out of Hyderabad and requires audit of SAP FLM (File Lifecycle Management). Service Provider shall produce deliverables as described in this ToR on a Fixed Price basis set forth in the Contract. Work will be performed on a hybrid model, visiting the Client Locations at Hyderabad and Kothagudem as required. The resource shall be reporting to the client on day-to-day activities and shall keep NISG informed (copy NISG) of all correspondences.

The following will be the scope of study.

1. Audit of File Type Creation & Workflow Triggering Mechanisms

This domain assesses whether file type definitions and trigger mechanisms are hardened against security risks.

A. Unauthorized File Type Creation Controls

- Assess whether controls exist to prevent unauthorized users from creating, modifying, or deleting file type definitions in the system.
- Verify that file type creation is restricted to authorized administrators only and requires a formal approval before activation.

B. File Type Configuration Security Review

- Review whether sensitive file types (legal, financial, HR, classified documents) have elevated security attributes — restricted access, enhanced audit logging.
- Assess whether file type metadata configurations expose sensitive internal classification logic that could be exploited (e.g., field names revealing internal coding schemes).
- Check whether file types allow unrestricted file format uploads (e.g., executable files, scripts) that could introduce malware into the document repository.

C. Workflow Trigger Security Assessment

- Assess whether workflow triggers can be manipulated by unauthorized users to initiate privileged actions (e.g., triggering an approval bypass, forcing a status change to "Completed").

- Verify that trigger conditions cannot be exploited through parameter tampering, injection attacks, or crafted metadata values.
- Identify triggers that fire without authentication verification — i.e., actions that can be initiated without confirming the identity of the requesting user.

D. Audit Logging of Events

- Confirm that trigger execution events — including actor identity, timestamp, file/record affected, and outcome — are fully logged.
- Assess whether logs are protected from modification or deletion by the same users whose actions are being logged.

2. Security Validation of Workflows

Security weaknesses in workflows — such as bypass routes, missing authentication steps, privilege escalation paths, or inadequate logging — can be exploited to circumvent approval controls, manipulate document lifecycle stages, or destroy records without authorization.

A. Workflow Bypass and Circumvention Testing

- Test whether workflows can be bypassed through direct table manipulation, batch input, BAPI calls, or RFC interfaces that skip the standard workflow routing.
- Assess whether any workflow steps can be completed without the required authentication or role verification.
- Identify workflows where a single user can initiate and approve the same action, creating a self-approval security risk.
- Test for the ability to force a workflow to a terminal state (approved/closed/disposed) without completing mandatory intermediate steps.

B. Authentication and Authorization Controls within Workflows

- Verify that every workflow step requiring approval or action enforces authentication of the acting user at the point of action — not just at login.
- Confirm that re-authentication or digital signature requirements are enforced for high-risk workflow steps (e.g., final approval).

- Assess whether workflow notifications (email, system alerts) include secure links and do not expose sensitive document metadata in plaintext.

C. Workflow Audit Trail Integrity

- Verify that workflow audit logs are complete, capturing every step, actor, timestamp, decision, and any overrides applied.
- Assess whether audit trail records can be altered, deleted, or backdated by workflow participants or administrators.
- Test whether failed workflow steps (errors, exceptions) are logged and generate security alerts where appropriate.

3. Security Review of Role-Based Access Control (RBAC)

Access control is the primary security layer protecting files and documents within SAP FLM. Weaknesses in role design, excessive access provisioning, SoD violations, and stale accounts represent the most direct path to unauthorized access, data manipulation, or insider threats. This domain constitutes the core security assessment of the application.

A. Authorization Object and Permission Security Analysis

- Conduct a detailed review of all authorization objects used within SAP FLM, focusing on objects that permit configuration changes, mass operations, or access to sensitive document categories.
- Identify authorization object values that are set to wildcard ("*") or overly broad ranges, providing effectively unrestricted access.
- Assess whether object-level security (access to specific document types, folders, or organizational units) is correctly enforced or can be circumvented.
- Review ACTVT (activity) values assigned per role to confirm that destructive actions (change, delete, archive permanently) are tightly restricted.

B. Segregation of Duties (SoD) Conflict Analysis

- Identify critical SoD conflicts including but not limited to: users who can both create and approve documents; users who can both initiate disposal and authorize it; users

who can modify documents and also manage audit logs; users who can administer roles and also hold operational access.
- Assess whether compensating controls exist and are effective for any SoD conflicts that cannot be technically resolved.

C. Privileged Access Security Review

- Identify all users with SAP_ALL, equivalent super-user profiles in the FLM environment.
- Review all system administrators, basis administrators, and FLM configuration users — confirm access is formally authorized, time-bound where applicable, and actively monitored.
- Review service accounts and batch/background user IDs used by SAP FLM for workflow automation — confirm they are locked for interactive use, have minimal necessary permissions, and passwords are managed securely.

D. Stale, Orphan, and Dormant Account Review

- Identify all active user accounts in SAP FLM belonging to terminated employees or transferred staff whose roles no longer require system access.
- Identify dormant accounts (no login within the past [90] days) that represent an unnecessary attack surface.
- Assess whether automatic de-provisioning controls are in place and functioning correctly upon HR-triggered separation events.
- Review shared or generic accounts and assess the security risk they pose due to lack of individual accountability.

E. Sensitive Data Access Review

- Identify which roles and users have access to the most sensitive document categories (e.g., legal case files, audit reports, HR records, and financial documents).
- Review whether data masking or field-level security controls are applied where users require partial access to sensitive documents.

F. Developer and Cross-Environment Access Security

- Verify that developers do not have access to the Production SAP FLM environment.
- Confirm that the transport management process prevents direct modifications to Production without passing through approved Development and Quality environments.
- Identify any user accounts with access spanning multiple landscape tiers (Development, QA, and Production simultaneously).

4. Security Review of Customizations

A. Security Risk Classification of Customizations

- Classify all customizations by security risk level (Critical / High / Medium / Low) based on their access to sensitive data, ability to modify system behavior, and interaction with security-relevant objects.
- Prioritize review of customizations that: bypass standard authorization checks, access sensitive tables directly, interact with audit logs or retention rules, or provide external system connectivity.

B. Authorization Check Security in Custom Code

- Review all custom ABAP developments (Z-programs, function modules, BAdIs) for the presence of AUTHORITY-CHECK statements at every point of sensitive data access or modification.
- Identify custom programs that read, modify, or delete FLM-managed documents without performing authorization checks — these represent direct privilege escalation vectors.
- Assess whether custom programs use hardcoded user IDs, passwords, or system credentials — a critical vulnerability enabling unauthorized access.
- Verify that custom code does not include hidden backdoors, debug-access overrides, or commented-out authorization checks left from development.

C. Audit Log Manipulation via Custom Code

- Identify any custom developments that write to, modify, or delete entries in SAP FLM audit log tables.

- Verify that no custom program can suppress audit log generation for specific events or users.
- Assess whether custom code introduces logging gaps — actions performed through custom transactions that are not captured in the standard audit trail.

D. Data Ex-filtration and Exposure Risks in Custom Code

- Review custom reports and download programs for unrestricted access to sensitive document data without authorization controls.
- Identify custom interfaces or RFC-enabled function modules that expose SAP FLM data to external systems without authentication, encryption, or data filtering.
- Assess custom email or notification programs to confirm they do not inadvertently transmit sensitive file content to unauthorized recipients.
- Review any custom archival or export programs for the ability to extract documents in bulk without authorization checks or audit logging.

E. Change Management Security Review

- Identify any customizations directly deployed to the Production environment without passing through the standard transport process — a significant indicator of unauthorized change or insider threat activity.
- Assess whether developers have the ability to directly activate or modify custom objects in Production — which would represent a critical security control failure.

F. Third-Party and Integration Security Review

- Review all custom integration points (RFCs, APIs, web services, middleware) for use of strong authentication (no hardcoded or default credentials), encrypted data transmission (TLS), and input/output validation.
- Assess whether third-party systems connected to SAP FLM are granted only the minimum necessary permissions and are subject to the same security standards as internal users.
- Verify that integration error logs do not expose sensitive document content, user credentials, or internal system paths.

4 Deliverables

i. Draft Assessment Report: T+3 weeks
ii. Final Assessment Report: T+4 weeks

T – Project start date

5 Timelines

The estimated period for this exercise will be 4 weeks.

6 Payment schedule

i. Engagement Kick off – 20%

ii. Submission of draft report – 50%

iii. Final report submission – 30%

7 Terms of Engagement

7.1 Response to this ToR:

i. The Service Provider must respond to this ToR by submitting the signed, sealed and scanned Form I (on company's letter head) along with duly filled, signed and sealed Annexure I & II through email on or before data and time mentioned in the data sheet. The responses shall be mailed to contacts mentioned in the data sheet. Complete responses, as required in this TOR, received within the above mentioned date and time, to the above mail-id, shall only be considered for evaluation. I

ii. Form I is the covering letter to be signed by the authorized person from the Service Provider.

iii. Annexure 1 shall be filled up with the details of the proposal and the total commercials for the project.

iv. The proposal should carry the following

- Project plan
- Resources to be deployed including their past experiences.
- Methodology
- Tools to be deployed, if any.
- Governance mechanism.

v. The commercials shall include all charges GST. Annexure 1 to be provided in a separate pdf file with password. Password will be requested from all the bidders who have technically qualified.

7.2 Evaluation

i. Technical Evaluation

The Technical evaluation will be done on the following parameters

Evaluation Criteria	Marks
1) Overall project Plan, Methodology, Tools - Meets the requirement – 15 - Doesn't meet the requirement - 0	15
2) SAP projects in similar nature - 2 = 20 - 1 = 15	20
3) Profile of consultants a) Project Manager: 25 - > 7 years SAP experience: 25 - 5 – 7 years SAP experience: 20 - 3 -5 years SAP experience: 15 b) Functional consultant GRC: 20 - > 2 projects in SAP GRC :20 - 1 project in SAP GRC : 15 c) Functional consultant SAP FLM: 20 - > 2 projects in SAP FLM :20 - 1 project in SAP FLM : 15	65

Bidders will have to score 70 or above to qualify Technically

ii. Commercial Evaluation

a) Commercial bids of all Technically qualified bids will be opened. The successful bidder will be decided on the Least cost basis.

b) The prices for Commercial evaluation will be considered excluding Taxes.

7.3 Work Order:

A work order would be issued to the selected service provider.

NISG reserves the right to withdraw or cancel or modify the Terms of Reference at any point *of time*.

8 Terms and Conditions

a. **Standard of Performance:** The service provider shall perform the Services and carry out their duties with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices. The service provider standards of performance and conduct shall be guided by the Client's requirements, defined Performance Standards and Code of Conduct.

b. **Line of Authority:** The resources of the service provider will report to the Client's nodal officer/ official indicated by client/ designated manager of the NISG, who will set the work priorities, the expected outcomes and the timelines. NISG will make payments to the Service Provider subject to the receipt of approval from the client. NISG may seek feedback from the client about the performance of the service provider, if required.

c. **Misconduct:** If "NISG" finds that any of the resources of the service provider has committed serious misconduct or has been charged with having committed a criminal action, or has reasonable cause to be dissatisfied with the performance of any of the resources, then the Service Provider shall, at the NISG's written request specifying the grounds thereof, within 10 working days, provide a suitable replacement candidate having qualifications and experience acceptable to the NISG.

d. **Status Reporting:** The resources may be directed to give a periodic status report by the client. The service provider will not be required to give similar reports to NISG, except when they are requested to do so to assess the status of the engagement and to strengthen the relationship with NISG.

e. **Insurance:** The service provider must make suitable arrangements for all the insurance needs of the service provider. NISG will not bear any liability whatsoever for the service provider, under any circumstances.

8.1 Replacement:

Except as "NISG" may otherwise agree, no resource selected for this engagement shall be changed, or replaced. If, for any reason beyond the reasonable control of the Service Provider, such as resignation, retirement, death, medical incapacity, disability among others, it becomes necessary to replace any of the resource, the Service Provider shall, within 5 working days, provide a suitable replacement candidate with equivalent or better qualifications. Any of the resources provided as a replacement above shall be subject to prior written approval by the "NISG". Also, the Service Provider shall bear all additional travel and other costs arising out of or incidental to any removal and/or replacement.

8.2 Confidentiality and Conflict of Interest:

The resources deployed at the NISG/Clients premises shall hold the "NISG's/Client's" interests paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments or their own corporate interests. If during the period of this contract, a conflict of interest arises for any reasons, the service provider shall promptly disclose the same to the NISG and seek their instructions.

8.3 Other terms:

a) The service provider must agree and abide by the rules and regulations applicable to consultants of NISG.

b) Any other out of pocket expenditure such as travel incurred for the engagement will be completely arranged for, by NISG. All boarding passes shall be submitted to NISG immediately upon completion of the travel.

c) The resources must be open to travel as required.

d) The resources should be available on email/phone for any ad-hoc support and contact.

e) The resources will also abide by all other guidelines/rules/regulations/instructions necessary/as applicable by/for NISG.

f) The documents and artifacts generated from this work/ assignment will be the sole property of client and should not be disclosed to any other entity without prior approval of the client. The service provider may be required to sign a Non-Disclosure Agreement in this regard, if required.

<u>FORM I</u>

(To be submitted on Service Provider's Letter head)

Place:

Date:

To

CEO
National Institute For Smart Government
New Delhi

Sir

Sub: Submission of response to the ToR for providing SAP consulting services – reg.

***

Having examined the Terms of Reference (ToR), we the undersigned, express our willingness, and hereby offer to provide the consultancy services mentioned in the terms of reference. We state that we shall abide by the provisions of the ToR.

Signature:

Name:

Designation:

Company Seal

Annexure 1

Details of the proposal – the bidder may submit in their own format.

Signature:

Name:

Designation:

Company Seal

ANNEXURE 2

Please attach the resume' of all the proposed key resources.