GEPF GOVERNANCE, RISK, AND COMPLIANCE SOLUTION - BID 06/2026

QUESTIONS	RESPONSES
Our solution has no physical servers, owned network infrastructure, or on-premises components. Each infrastructure layer is operated by an enterprise cloud vendor whose own security programme includes continuous independent penetration testing. In this context, could GEPF clarify what specific components or layers are intended to be covered by the penetration testing requirement?	The RFP specifies that "the solution and hosting environment must support vulnerability management and penetration testing. Bidders must provide evidence of recent penetration testing and remediation practices and confirm the ability to support independent penetration testing by GEPF, or its appointed service providers where required." In your context (cloud-hosted solution): • **Application Layer**: Penetration testing must cover your GRC application itself — including modules, workflows, integrations, and configurations. Evidence should demonstrate that vulnerabilities are tested and remediated. • **Hosting Environment**: Since infrastructure is operated by your cloud vendor, penetration testing at this layer is satisfied through the vendor's own independent testing programme. Certificates or attestations confirming scope and remediation practices are acceptable substitutes for raw test results. • **Independent Testing:** GEPF reserves the right to conduct or commission independent penetration testing. You should confirm that both your application and the cloud environment can accommodate this, even if the cloud vendor limits direct access to raw results.

GEPF GOVERNANCE, RISK, AND COMPLIANCE SOLUTION - BID 06/2026

Whether vendor SOC 2 Type II certifications — which are subject to continuous independent audit — satisfy the intent of the information security requirement at the infrastructure layer?	The RFP requires compliance with recognised standards: "Compliance with Data Privacy laws/legislation amongst others POPIA, PAIA, Cybercrimes Act, and recognised security standards (ISO 27001 / SOC 2 / NIST)." A SOC 2 Type II certification at the infrastructure layer does satisfy the intent of the information security requirement. It demonstrates continuous independent audit of controls, including security and availability. However, certification alone is not sufficient. You must also provide evidence of penetration testing and remediation practices (via certificates/attestations) and confirm compliance with South African data residency and privacy laws.
Could you kindly confirm the number of users who will use the software (to provide accurate pricing).	We confirm the following licensing requirements: • 10 fully licensed users, including 2 System Administrators; and • 31 limited users.
Could you kindly confirm whether data migration from the existing system will form part of the implementation?	There will be no data migration from the existing system. The new solution will be implemented as a fresh deployment, and no historical data is required to be migrated.
We kindly request a copy of the attendance register/proof of attendance for the compulsory briefing session held yesterday, 01/07/2026 at 10:00, in relation to the tender titled RFP for the Appointment of a Software Service Provider to Provide a	As indicated in the meeting, the GEPF will utilize the MS Chat box and the attendance register generated from the meeting to confirm the attendance of the bidders.

GEPF GOVERNANCE, RISK, AND COMPLIANCE SOLUTION - BID 06/2026

Governance, Risk and Compliance Solution – GEPF 06/2026, as this is required for our bid submission.	