TERMS OF REFERENCE

Implementation of Privileged Access Management (PAM) and Identity & Access Governance (IAG)

1. Background

The organisation intends to strengthen its cybersecurity posture by implementing an integrated Privileged Access Management (PAM) and Identity & Access Governance (IAG) solution. The current environment consists of multiple identity systems, limited control over privileged access, and fragmented governance processes, which create security, compliance, and operational challenges.

To address this, the organisation seeks a single, integrated solution or a tightly unified platform capable of managing identities, access, and privileged accounts across both on-premises and cloud environments.

2. Objectives

The primary objective is to implement a centralised identity security platform that manages user identities and controls privileged access effectively. The solution must ensure that only authorised users have access to systems and data, enforce least privilege principles, and provide complete visibility and auditability of access activities.

In addition, the system must automate identity lifecycle processes, support compliance requirements, reduce risks associated with privileged access, and eliminate reliance on multiple standalone tools.

3. QCTO'S CURRENT ICT LANDSCAPE

1. The QCTO has one site situated in Hatfield, Pretoria. The current ICT infrastructure and system supports about 150 staff across the different departments.
2. The QCTO currently utilises a Security Information and Event Management (SIEM) solution, Seceon
3. The QCTO ICT unit provides various ICT services on different infrastructure platforms and systems products.
4. The QCTO has a local network of about 150 end user workstations, Four (4) HP physical servers that are hosting (17) virtual machines running Windows operating systems and four (4) Cisco switches.

4. Scope of Work

The appointed service provider will be responsible for the design, supply, implementation, and configuration of a PAM and IAG solution. The solution must support deployment in cloud, on-premises, or hybrid environments and integrate with the organisation’s existing systems such as Active Directory, enterprise applications, and cloud platforms.

The scope includes the configuration of identity governance processes such as access requests, approvals, and periodic access reviews, as well as the implementation of privileged access controls including credential vaulting, session monitoring, and just-in-time access.

The vendor will also be required to migrate relevant existing data, retire redundant systems where applicable, and ensure minimal disruption to business operations during implementation.

4. Functional Requirements

The proposed solution must support identity lifecycle management processes including onboarding, role changes, and offboarding. It must enable automated provisioning and deprovisioning of user access, enforce role-based and policy-based access controls, and support segregation of duties controls.

From a privileged access perspective, the system must provide secure management of privileged accounts, enforce strong authentication, and allow controlled and auditable access to critical systems. It must also provide full visibility of privileged sessions, including monitoring and recording capabilities.

5. Technical Requirements

The solution must be scalable, secure, and capable of operating in a hybrid IT environment. It should integrate seamlessly with existing identity stores and enterprise systems and support standard authentication protocols such as single sign-on and multi-factor authentication.

The platform must provide a centralised dashboard for monitoring, reporting, and administration, and must allow integration with other security tools such as SIEM platforms. High availability and performance must be ensured.

6. Deliverables

The vendor will be expected to deliver a complete solution including system architecture, implementation plan, configured system, and integration with identified platforms. Documentation covering system design, administration, and user guidance must be provided.

Training sessions for administrators and end-users must be conducted, and support must be provided during system testing, go-live, and post-implementation stabilisation.

7. Roles and Responsibilities

The vendor will be responsible for the overall implementation, integration, configuration, and knowledge transfer. The organisation will provide access to systems, assign internal resources, and participate in validation, testing, and approvals.

Both parties will collaborate throughout the project lifecycle to ensure successful delivery.

8. Project Timeline

The project is expected to follow a structured implementation approach beginning with planning and design, followed by system deployment, integration, testing, and final rollout. The estimated duration for the full implementation is approximately three to six months, depending on complexity.

9. Evaluation Criteria

Proposals will be evaluated based on the vendor's ability to deliver an integrated PAM and IAG solution, relevant experience, technical capability, scalability, and alignment with industry standards. Consideration will also be given to cost, support model, and track record of similar implementations.

Evaluation Criteria

Stage	Criteria	
1	**Detailed Curriculum Vitae (CVs) of Key Personnel (20 Points)** Bidders must submit detailed CVs of all	**Relevant skills & experience (IAM, IGA, PAM, cybersecurity, integration) 8** **Certifications (minimum required met) 4**

	key personnel assigned to the project, clearly indicating qualifications, certifications, and relevant experience. The proposed team must demonstrate skills and experience in the following areas: • Identity & Access Management (IAM), Identity Governance (IGA/IAG), and Privileged Access Management (PAM) • Cybersecurity architecture and enterprise security implementation • System integration, including Active Directory, cloud platforms (e.g., Azure/AWS), and enterprise applications • Security compliance and governance frameworks (e.g., ISO 27001, NIST, Zero Trust) • Project management and delivery of enterprise security solutions **Minimum certification requirements:** • At least one (1) team member must hold a relevant professional cybersecurity or information security certification (e.g., CISSP, CISM, or CISA) • At least one (1) team member must hold a certification related to Identity and Access Management or cloud security (e.g., Microsoft Identity/Entra, Azure Security, or equivalent) **Preferred certifications (advantageous):** • Product-specific certifications (e.g., CyberArk, Saviynt, SailPoint, or equivalent PAM/IGA platforms) • TOGAF or equivalent enterprise architecture certification • ITIL Foundation or higher	**Additional / preferred certifications (advantage) 4** **Team composition & role alignment (fit for project scope) 4**

	Copies of all certifications must be provided as proof.	
2	**Project Experience and References (20 Points)** Bidders must submit at least four(4) signed and dated reference letters from clients for projects of a similar nature completed within the last three (3) years. The reference letters must clearly indicate project scope, duration, and confirmation of successful delivery. Preference will be given to projects involving Identity Governance, Privileged Access Management, or integrated identity security solutions within medium to large organisations.	**Number of valid reference letters (4 or more reference letters) 20** **Number of valid reference letters (2-3 reference letters) 10** **0 reference letters 0**
3	**Project Proposal** (25 Points) Bidders must submit a detailed project proposal outlining their approach to implementing the proposed Privileged Access Management (PAM) and Identity & Access Governance (IAG) solution. The proposal must include: • Understanding of the organisation's requirements and objectives • Proposed architecture and solution design (including PAM and IGA components) • Implementation methodology and phases (design, deployment, integration, testing, go-live) • Integration approach with existing systems (e.g., Active Directory, cloud platforms, enterprise applications) • Project timelines and key deliverables • Risk management and mitigation approach	**Excellent Project Plan and Proposal covering all elements = 25 points** **Average Project Plan and proposal covering some elements = 08 points ·** **Mediocre Project Plan and proposal = 02 Points ·** **No project and proposal = 0 points**

	• Post-implementation support and knowledge transfer	
4	OEM Partner letter (10 Points) Bidders must provide a valid and current Original Equipment Manufacturer (OEM) or authorised partner letter confirming, partnership or authorisation status	**Valid Partner letter 10** **No Partner letter 0**
5	**Sample System Reports (25 Points)** Bidders must provide sample or anonymised reports generated from the proposed solution, demonstrating system capabilities. Reports must: • Demonstrate auditability, traceability, and compliance • Be clear and professionally structured • Be submitted as screenshots or exported formats (PDF/Excel)	**Comprehensive, clear, and professionally structured reports demonstrating strong system capabilities, including auditability, traceability, and compliance. Submitted in correct format and easy to interpret** **25 Points.** **Reports provided but lack clarity, completeness, or sufficient demonstration of required capabilities.** **10 Points** **No reports submitted or reports are not usable/irrelevant.** **0**

Bidders must achieve a **minimum score of 80 out of 100 points** to be considered for further evaluation or award.

ENQUIRIES

For further information, please contact the following QCTO staff members:

Technical enquiries can be directed to:

Mr Hangwelani Tshifaro
Tel no: 012 003 1829
Email: Tshifaro.h@qcto.org.za