**GPAA Customer Questionnaire**

**Technical:**

1. Which non-information technology departments and systems need to work with the identity management system?

For example, human resources, physical security, finance? Do they already have information or systems in place that will help the initiative?

*Benefits payment (core business), Human Resources, finance, Supply Chain, Physical Security.*

*For Human resources we use Persal which is a transversal system hosted by SITA. However GPAA is in a process of implementing a new internal HR system. For finance and supply chain we use ACCPAC.*

1. What business processes need to be put in place to support identity management?

*User access provisioning – that includes user access creation, allocation of rights and privilege*

*User access de-provisioning and archiving of unused access accounts.*

Who will create, implement and manage the processes?

*The creation of processes will be performed by GPAA in conjunction with the successful supplier. The supplier will implement the process onto the system during the project phase. Once the project is handed over to production it will be performed by GPAA as part of business as usual activities.*

1. Which of the below features of identity management will the proposed solution should be implemented primarily in Phase 1?

*User access provisioning, identity life cycle management, role-based access control, Privileged Account Management*

1. How will users be de-provisioned so there are no orphan accounts?

*Users will be archived after a particular period following the de-provisioning of those accounts. The de-provisioning will either be user initiated (e.g. when a person resigns) or through system monitoring e.g. when the account is inactive for a particular period.*

1. Who is responsible for Role Mining (Defining roles based on Business Roles/Job functions)?

*It’s GPAA ICT by using the requests from Business and Human Resources. Most roles have already been defined in our legacy system which runs on mainframe. These roles/definitions will be migrated to the new system.*

1. Besides GPAA employees, who else needs access — general-public, vendors, contractors, state and local agencies?

*It will be Employers (e.g. department of education or home affairs) who lodge applications for pension on behalf of their employees. It will be also the members of the fund and this will be for self-service purposes.*

1. What types of physical components need to be integrated?

*For now it will be for biometrics solutions*

1. What are the primary solutions expected as part of the Phase 1?
   1. *Both Identity Management & Access Management?*
2. Is Identity Governance (Access Certifications & Attestation) Part of Phase1?

*Yes*

1. Is Fine Grained application authorization using XACML part of Phase 1?

*Yes*

1. Is external user's (Partners/Traders) authentication (Federation) Part of Phase 1.

*Yes – employers and members of the fund.*

1. Is Device/Risk Score based Authentication (For securing Financial Transactions) is part of Phase1?

*Yes*

1. No. of users (Internal/external) need to be supported by IAM System for Phase:

*About 1500 internal users and 1,3 million for external users*

1. What are the Information Security Compliance Standards (COBIT, ISO 270001, NIST) already in Place for GPAA with which the proposed solution need to be complaint?

*We have adopted COBIT, ITIL and ISO 27000 as our guiding standards and frameworks.*

1. What are the Financial Security Compliance Standards (SOX, GLBA) already in Place for GPAA with which the proposed solution need to be complaint?

*We are required to compliant to SA legisations. We are not required to comply to external legislations such as SOX or GLBA*

1. What are the Cyber Security Preventive Standards (CFAA, ITADA) already in Place for GPAA with which the proposed solution need to be complaint?

*None of these at the moment. However this will form part of future information security strategy for GPAA and the solution should be able to cater for such requirements when GPAA decides to implement them.*

1. Are there any requirements for SIEM (Security Incident and Event Management) to be part of the Proposed solution?

*No. We have implemented a separate SIEM solution.*

1. Is Mobile Integration with IAM System is part of Phase 1?

*Yes.*

1. Are there any requirements for Social authentication and Integration (With Facebook, Twitter, etc..) to be part of the Proposed solution?

*Yes, however in the next phases of the project.*

1. Is there any suggested/preferred methodology from GPAA for IAM implementation (RUP, OUM, Agile)?

*We subscribe to Agile approach for all GPAA projects.*

1. Does the IAM Solution be hosted in the GPAA datacentre or by Vendor established datacentre?

*At the GPAA datacentre.*

1. Are Business Continuity Processes (BCP) for Disaster Recovery part of the Proposed Solution for Phase 1?

*Yes in a sense that the solution must cater for high availability requirements.*

1. Are there any Tools available with GPAA for Source Control, Build & Release & Deployment Automation Tools?

*Yes, they are used by the development team.*

1. Are there any Tools available with GPAA for Software Development, ITSM process management?

*Yes, they are used by the development team.*

1. Are there any requirements for GPAA to have the integration of IAM Solution with Business Intelligence Reporting tools?

*Yes.*