APPENDIX-E

SERVICE LEVEL AGREEMENT (SLA)

1. PURPOSE

The purpose of this Service Level Agreement (SLA) is to specify in detail the level of maintenance and support service expected from the Supplier under the Contract for the supply, installation, training and maintenance of Integrated Platform for Risk Assessment, of which this SLA is an integral part. This SLA will evolve over time, with additional knowledge of the Bank's requirements, as well as the introduction of new applications and services into the support portfolio provided by the Supplier.

2. SCOPE OF THE SLA

2.1 Services Provided

The following services shall be provided:

2.1.1. **Preventive maintenance** - All software shall undergo regular maintenance works with a view to undertaking corrective preventive maintenance actions. The frequency and content of such preventive maintenance activities shall be proposed by the Supplier and approved by the Bank within ten (10) days of the signing of this contract. The latter reserves the right to modify the proposal to better reflect its needs. In any event these activities shall include, among others, the identification, analysis and actions aimed at preventing the occurrence of potential problems.

2.1.2 **Corrective maintenance** - Defined as activities associated with root-cause analysis and bug-fix isolation and resolution.

2.1.3 **Root-cause analysis** - Analysis of the root causes of problems. Problems will be reviewed to determine their root causes, measures will be taken to correct the sources of the problems, and reports will be prepared and distributed in a timely fashion.

2.1.4 **Bug fixes** - Defined as the emergency repair of any system operation that does not comply with the current signed and approved system specification. This includes system errors, "hung" or halted screens, or unexpected results within the system that render it unusable for the purpose for which it was designed.

2.1.5 **Adaptive maintenance –** The Supplier shall provide adaptive maintenance that is activities relating to upgrades or conversions to an application due to new versions of operating environment, including operating system, application server, or database software.

2.1.6 **Advice of Performance** - The Bank's Security unit will inform the Supplier of the resolution of each problem brought to its attention by e-mail.

2.2 Other Services

The following hardware and software application-related services shall also be provided:

2.2.1 **Application monitoring** – The Supplier will make every effort to conduct **upon Bank's request;** periodic monitoring of the system performance to determine whether there is deterioration and advice the Bank on the same.

2.2.2 **Transition of new or modified applications -** When a new or modified application is ready to be transitioned into support, planning and coordination of the necessary activities between the Bank's Security unit and the Supplier's support team will be conducted by the Bank's Security unit. Other requirements include:

- Support will commence for new or modified software immediately after deployment.
- The Supplier shall make available to the Bank the required support resources (human and other) to provide knowledge transfer for a period of 60 days after deployment of new software and/or upgrade.

2.2.3 **Status reporting** - monthly status reports will be completed by the Bank's Security unit and submitted to the Supplier for all items covered by the Maintenance Contract. Monthly Status reports will be discussed by the Bank's Security Manager or the Bank's Chief Information Security Officer with the Supplier's Support management to ensure that the Supplier is aware of the support issues and risks faced by the Bank.

2.2.4 **Knowledge management** - Recording, storing, and retrieval of information to assist in the resolution of problems will be established by the Supplier and maintained by the Bank.

2.2.5 **Software licensing -** Pursuant to the general conditions of the Supply, Installation and Commissioning of Hardware Equipment and Software, the Supplier shall provide all software together with the licensing appropriate to the Bank's operations.

2.2.6 **Specific training** – The Bank may purchase and Supplier shall provide training for the Bank's Security Team Members. The Supplier shall provide advice and training about the solution and its integration into the Bank's IT environment.

2.2.7 **Upgrades to application software -** When an upgrade to the system is released i.e. operating system drivers, firmware upgrades, and vendor-required upgrades; the Supplier shall provide and install the upgrade at no additional cost to the Bank.

3. PROCESSES AND PROCEDURES RELATED TO THIS CONTRACT

3.1 ***Request for Support***

A request for support is defined as a request to fix a defect in existing software application and/or hardware or a malfunction in the security system as a whole. Such

requests may be executed by e-mail, fax or phone call. In the latter case the Bank's Security unit must summarize in writing for its file, the conversation held with the Supplier and/or its Local Agent. The support request sent to the Supplier shall clearly mention the severity level of the problem.

3.2 *Call Management Process*

The Supplier shall set up within its organization a unit in charge of recording and tracking all problem reports, inquires, or other types of calls received from the Bank.

3.3 *Performance Evaluation*

3.3.1 *Evaluation Reporting*

The Bank will provide regular reporting to the Supplier to indicate how the latter is performing vis-à-vis the related target performance (see below). These reports are expected to be produced by the Bank's Security unit and will provide details on the Supplier's performance against SLA targets.

3.3.2 *Evaluation Criteria*

Reporting against the SLA resolution targets will focus on the time to resolve operating problems. This evaluation will only address the support requests submitted to the Supplier for resolution. The evaluation report will be in the form of a written letter or e-mail as appropriate.

4. CHARACTERISTICS FOR PROBLEM CATEGORIZATION

4.1 Severity Codes

The following characteristics are used to identify the severity of a problem report:

- Business and financial exposure
- Work outage
- Number of clients affected
- Workaround
- Acceptable resolution time

It is not necessary (nor is it likely) to have perfect match of each characteristic to categorize a problem report at a particular severity level. A given problem must be judged against each of the characteristics to make an overall assessment of which severity level best describes the problem.

Severity 1 (Critical)	Severity 2 (High)	Severity 3 (Medium)	Severity 4 (Low)
Business and financial exposure			
The hardware/application failure creates a serious business and financial exposure.	The hardware/application failure creates a serious business and financial exposure.	The hardware/application failure creates a low business and financial exposure.	The hardware/application failure creates a minimal business and financial exposure.
Work Outage			
The hardware/application failure causes the client to be unable to work or perform some significant portion of their job.	The hardware/application failure causes the client to be unable to work or perform some significant portion of their job.	The hardware/application failure causes the client to be unable to perform *some small* portion of their job, but they are still able to complete most other tasks. May also include questions and requests for information.	The hardware/application failure causes the client to be unable to perform a *minor* portion of their job, but they are still able to complete most other tasks.
Number of Clients Affected			
The hardware/application failure affects a *large* number of clients.	The hardware/application failure affects a *large* number of clients.	The hardware/application failure affects a *small* number of clients.	The hardware/application failure may only affect one or two clients.
Workaround [This bullet carries the heaviest weighting of the characteristics for Severity 1 and 2.]			
There is no acceptable workaround to the problem (i.e., the job cannot be performed in any other way).	There is an acceptable and implemented workaround to the problem (i.e., the job can be performed in some other way).	There may or may not be an acceptable workaround to the problem.	There is likely an acceptable workaround to the problem.
Response Time			

Severity 1 (Critical)	Severity 2 (High)	Severity 3 (Medium)	Severity 4 (Low)
Within one hour.	Within one hour.	Within eight hours or by next business day.	Within eight hours or by next business day.

4.2 Levels of Service

The service levels offered by the Supplier to the Bank are described below. The Supplier's goal must be to meet, and even exceed, when possible, the levels of services described below:

Service Level	Severity 1, 2	Severity 3, 4
24/7	- The Supplier and/or Local Agent shall provide support 24 hours, seven days a week by phone and/or on-site intervention by operations and application specialists. - Support requests are taken 24 hours, seven days a week. - Telephone call back within one hour from receipt of the request by the Supplier and/or Local Agent. Guaranteed shipment of hardware replacements within one (1) business day of receiving the request for support.	- Requests taken 24 hours, seven days a week. - The Supplier and/or Local Agent shall provide support during normal working hours in the Bank, by phone and/or on-site intervention. - Call back within one hour during normal working hours at the Supplier or Local agent. - Guaranteed shipment of hardware replacements within one (1) business day of receiving the request for support.

4.3 Levels of Effort

The level of effort expected of the Supplier shall be exercised in full, either through corrective maintenance activities or through preventative maintenance activities.

5. ROLES AND RESPONSIBILITIES OF THE BANK AND THE SUPPLIER

5.1 The Supplier

The Supplier's Support Team has the following general responsibilities under the Contract:

- The Supplier shall conduct business in a courteous and professional manner.
- Once a support request has been submitted, the Supplier shall make itself available to work with the Bank's support resource assigned to the support request.

- The Supplier shall continue to provide the Bank access, software, licensing, training, documentation, and support for all software and hardware supplied.
- The Supplier shall provide all of the necessary and requested documentation, information, and knowledge capital to the Bank prior to the deployment of any new application.

Supplier's Support Specialists

- The Bank end-users do not contact the Supplier support resources directly to report a problem. All problem calls must be logged through the Bank's Security unit.
- Conducting all root-cause analysis and bug fix isolation and resolution activities, and associated documentation for the individual tasks, as assigned by the Bank.
- Acting as a point of contact for all application issues (bugs and enhancements).
- For enhancements, determining the potential high-level effort for all changes, and based on that, either passing it on to a developer or completing it themselves.
- Identifying all tasks associated with each support request and deriving estimates for the completion of each task.
- Responsible for responding to support requests.
- Conducting coding and testing to resolve application problems.
- Participating in the acceptance testing and implementation activities.
- Providing knowledge transfer to the Bank's Security unit staff.
- Preparing status reports upon request.

5.2 **The Bank**

The Bank has the following general responsibilities under the Contract:

- The Bank shall conduct business in the context of this Contract in a courteous and professional manner with the Supplier.
- The Bank shall log all information from the Supplier required to establish contact information, document the nature of a problem and the Supplier's hardware/network environment (as applicable).
- The Bank shall attempt to resolve problems over the phone on first call.
- The Bank shall escalate support request to next level of severity upon approach of established resolution targets.
- The Bank's Security unit shall assign severity codes based on its analysis of the situation.

There are several roles deployed within the Bank that are integral to the provision of support services to the Bank. These roles include the following:

Bank's Security Unit

Chief Risk Infrastructure Officer

The Bank Chief Risk Infrastructure Officer works as a point of contact for all activities relating to the transition of a new or modified application from the Supplier to the Bank's Security unit and the decommissioning of supported applications. Reporting to

the person in charge of the Bank's Security unit, he/she is responsible for planning, coordinating, and overseeing the transition of a new application into support. His/her duties include:

- Liaising with the Supplier's support team head.
- Ensuring all required documentation, information, and knowledge capital has been prepared, as per transition checklist, and turned over prior to the start of support for a new application.
- Managing all activities relating to transition:
  - Identifying resource requirements, including Level of effort and technical skills.
  - Identifying all access requirements and tools required.
  - Meeting with the Supplier's team or Local Agent to set up timetable and develop transition plan.
  - Developing training plan for the Bank's Security unit.
  - Negotiating resource assignments with the person in charge of the Security unit or the Chief Information Security Officer.
- Creating and ensuring currency of Support Applications Repository.

Chief Risk Infrastructure Officer

The Bank's Chief Risk Infrastructure Officer will provide the overall direction of the activities of the support specialists, participate directly in the production of the associated deliverables, and will negotiate with the Supplier's support manager regarding the classification of enhancements and the scheduling of tasks. His/her duties will include:

- Ensuring SLA targets are met (coordinating all activities to ensure all tasks are performed in a consistent manner and on schedule).
- Ensuring all work is performed according to the agreed-upon work methods and standards.
- Participating directly in the production of the associated deliverables.
- Assigning severity codes to support requests and liaising with the Supplier's team to negotiate the scheduling of tasks, and coordinate the activities of the Supplier's support team.

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be duly executed in their respective names by their duly authorized representatives, on the respective dates specified below.

FOR AFRICAN DEVELOPMENT BANK

_____

……
…….
CORPORATE PROCUREMENT DIVISION (CGSP.2)

_____
Date

FOR …….

_____

……..
GENERAL MANAGER

_____
Date