REQUEST FOR PROPOSAL

RFP AGRA-NB-1091

CONSULTANCY FOR IMPLEMENTATION OF AN ENTERPRISE RISK MANAGEMENT (ERM) SYSTEM

Disclaimer: AGRA reserves the right to determine the structure of the process, number of shortlisted participants, the right to withdraw from the proposal process, the right to change this timetable at any time without notice and reserves the right to withdraw this tender at any time, without prior notice and without liability to compensate and/or reimburse any party.

1. Background

AGRA is an African institution, founded and led by Africans and with roots across the continent. AGRA was founded by former UN Secretary-General the late Kofi Annan with funding from multiple international partners, in response to the need for an African institution to drive agriculture transformation across the continent. At AGRA, we understand that African farmers need uniquely African solutions, designed to meet their specific needs and environments to sustainably increase production, and gain access to rapidly growing agriculture markets.

AGRA's mission is to catalyze transformational change in agriculture across Africa, and to improve the lives of millions of smallholder farmers. AGRA's three headline goals are: to directly reach 9 million farmers, to indirectly reach 21 million farmers with best-bet agricultural technologies and practice, and to help advance 11 countries on their inclusive agricultural transformation (IAT) pathways. AGRA work with African partners, who identify and deploy approaches that are appropriate to the continent and are alive to the local context. AGRA collaborate with African governments, with whom it partners and help them implement the priorities and policies contained in their national agricultural development strategies.

AGRA recognizes the critical importance of effectively managing and mitigating risks to achieve its strategic objectives. To enhance the risk management process, ERC intends to implement an Enterprise Risk Management (ERM) processes automation system. The system will enable the organization to streamline risk identification, assessment, monitoring, and reporting activities, thereby improving decision-making and overall risk management capabilities. The purpose of this Terms Of Reference is to outline the objectives, scope, and key deliverables of the ERM processes automation project.

2. Scope of Work

The ERM system will provide features and functionalities that fully automate the full end-to-end risk management processes at AGRA: Key system functionalities are:

- The system should be able to allow for capture and segregation of data by various entity types such as subsidiary companies, organizational units, programs, countries, divisions, and departments.
- The system should have access controls capabilities that allow – users' access assignment across specific or all entities.
- Ability to support various risk management frameworks, such as COSO ERM, ISO 31000, or industry-specific standards, and allow customization to meet organizational requirements.

- The system should provide configurable reporting capabilities, dashboards, risk heat maps, trend analysis, and ad-hoc reporting to meet diverse stakeholder requirements.
- Easy to use and user-friendly user interface with easy progression from phase to phase.

Functional Requirements

- Risk Identification: The system should allow for the capture and updates of identified risks across various organizational units, countries, programs, divisions, and departments. It should support the capture of risk events, risk sources, and associated control measures.
- Risk Assessment: The system should facilitate the assessment of risks based on their impact and likelihood. It should provide a standardized methodology for risk scoring and prioritization.
- Risk Register and Repository: The system should offer a centralized database to store and manage risk information and classification of risks based on categories, impact, and likelihood, as well as the ability to track risk ownership and accountability.
- Risk Mitigation Planning and Tracking: Should have workflow capabilities for creating and monitoring risk mitigation plans, assignment of responsibilities, implementation dates, progress tracking and reminders for tasks according to defined trigger points.
- Risk Monitoring: The system should enable the continuous monitoring of identified risks. It should allow for the tracking of risk mitigation actions, monitoring of key risk indicators, and automatic notifications of critical risk events.
- Reporting and Analytics: The system should enable generation of comprehensive and customizable risk reports and dashboards. It should provide robust analytics and visualization tools to aid in decision-making.
- Risk Appetite and Tolerance Framework: The system should enable specification of risk appetite and tolerance levels and monitoring and reporting on risks exceeding defined thresholds.
- Incident and Issue Management: Offer capabilities for escalation mechanisms for significant risks and system for reporting and tracking risk-related incidents and issues through escalation and notification mechanisms and collaboration features for incident resolution.
- Integration: The system should integrate with existing organizational systems, such as the audit management system, to ensure seamless data exchange and avoid data duplication.
- Security and Access Control: The system should incorporate robust security measures to protect sensitive risk-related information. It should allow for role-based access control to ensure appropriate access rights for different user groups.
- High Impact Risk Register Log: Maintain a risk register log for high impact risks across the organization and integrate with the audit management system (teammate+).

Non-functional and Technical Requirements

Integration and General Requirements

The system should have the necessary integration capabilities that will allow it to work with key elements of a service-oriented driven architecture that includes:

- System to support Service Oriented Architecture (SOA)
- Provides multi-lingual capabilities, in particular, English, French and Portuguese
- dedicated process management tool that ideally controls processing and sequencing of orders across various systems to facilitate interoperability of applications.
- messaging bus that handles communication between applications to facilitate interoperability of applications.
- Reports on failed transactions and recognize transaction failure notification from external systems as communicated by the messaging service bus.
- The proposed solution must provide comprehensive and easily accessible on-line help facilities to the users.
- Provides extensive reporting capabilities, including in-built report generation tools.
- Generates information that is compliant with generally accepted protocols/formats and standards, for consumption and use by an external BI and DW tool.
- Supports and enforces compliance through a detailed audit trail of every transaction- (user information and transaction history data)
- Supports a 24X7 availability.
- Can support a modular architecture that corresponds to the business processes in order to support a phased implementation.
- Supports fault tolerance.
- Integrates with a secure inbound and outbound email messaging platform.
- Provides integrated error and exception handling capabilities.
- Tracks business rules parameters for different time periods
- Permits the "posting" of data transactions in real time.
- The system can "roll back" non-committed transactions in the event of a system failure.
- Supports centralized process scheduling mechanisms.
- Ensures that the failure of any end user devices, e.g., workstations, printers, does not impact the operation or performance of other devices.
- Provides failover management capabilities for both application and database server.
- Can support a maximum latency of not more than one second for all acknowledgements, and, not more than 5 seconds for final delivery.
- Supports the assignment of priority to system functions (search, exports, backup)
- Provides validity checks on data elements at the point of data entry.
- Facilitates rapid data entry for large volume or high-speed data entry requirements.
- Allows automatic saving of work in progress.
- Allows the user to resume work in progress and also modify previously saved work in progress.
- Supports and executes structured workflows and allows the design and customization of workflows (around both processes and transaction types)
- Can embed SLAs within process workflows and supports SLA management (for example turn-around time for transactions), monitoring and reporting at individual transaction type level.
- The system should be able to work with outbound mail to communicate SLA non-compliance.

- Allows for development and customization of data capture/UI forms, including definition of parameters at form object level to enhance integrity of data capture on the various forms.

Enterprise Requirements

Security Concept

- The vendor will be required to provide a documented security design for the system.
- The security concept shall include:
  - an explanation of the system architecture, describing how the functional components are distributed / localized in the architecture, the standard platforms (e.g., hardware, OS, middleware, applications, and databases.
  - interfaces with other systems/applications and protocols.
- All installed & uninstalled components or applications shall be documented in the security concept.
- All supplier related Operations and Maintenance Procedures and roles shall be documented in the security concept.
- All remote maintenance procedures shall be stated in detailed documentation and are subject to ongoing security audits.
- All implemented and available authentication and authorization mechanisms shall be documented in detail, whether the features / functions are enabled or disabled, used or unused.
- The security mechanisms, available to secure the system against unauthorized use, manipulation, or disclosure of information on all application tiers shall be documented.
- An exhaustive list of all the installed security patches and modifications shall be supplied.
- The requirements of the system concerning security of the network infrastructure (e.g., firewall ports, DMZ configurations. etc.) shall be documented.
- User password requirements (e.g., minimum password length, maximum password lifetime, screen lock timeout, password complexity, maximum number of failed login attempts) shall be documented.
- An explanation of the concept used to archive log files in a trustworthy way for a configurable period of time according to resources and requirements shall be documented.
- Backup recommendations shall be provided by vendor and validated.
- Protocols/services which use random or dynamic network ports or port ranges are not allowed.
- The system shall have standards-based interfaces, at both the protocol and data representation levels, in order to facilitate operating within a security framework. All protocols shall be compatible with Firewalls, Network Address Translation and DNS.
- Interfaces and Protocols shall provide encryption and authentication based on industry-recognized standards.
- Ability of the Identity Directory to support authentication of users via Windows AD SSO, SAML tokens or Integrated Security.

Security and Integrity

- There shall be measures to safeguard against user error and fraud (i.e., system must check the validity of data entered into the system or imported from other applications.
- Critical / Confidential data shall not be stored anywhere where it could be at risk and shall be able to be encrypted whilst stored or transmitted (for example, encrypt credit card details stored in a database).
- The passwords used or required for the administration and for the operation of the system shall NOT appear in plain text in any file, or database.
- The system shall provide a granular access control mechanism that will determine functionality and data which users of various roles can have access to read write and execute. The principle employed should be that of "Least Privilege".
- System menu and screen functionality shall be based on a policy where, by default, no one is allowed to access anything, unless explicitly permitted so.
- All passwords shall be stored hashed or in a one-way encrypted form that is inaccessible by all users. They shall not be written in any file or database (i.e., log or cookie, cache, etc.).
- End User (including customer) passwords shall be inaccessible by any kind of user.
- Administrators will only be able to reset a user’s password but not be able to see a user's password.
- The system must not have any hard-coded passwords (i.e., service/application user passwords displayed in source code)
- End users shall be able to change their own passwords (provided the previous password is known) without requiring intervention of system administrators.
- The system shall enforce strength of passwords. System must provide a configurable mechanism to detect and block simple passwords.
- The system shall provide the capability to lock/deactivate/suspend or delete certain accounts/user IDs either manually or automatically, given some predefined actions/criteria (e.g., period of inactivity, defined number of failed logins attempts etc).
- The system shall provide the capability to extract and print a list of all possible access privileges.
- The system shall provide the capability to extract and print a specific user’s access privileges.
- All users shall be allocated a unique user ID for the sole use of the individual. The system must not have functionality that requires generic user accounts.
- The number of unsuccessful log-on attempts shall be limited to a configurable number of attempts per session; afterwards, the session will be terminated.
- Remote operation and maintenance tasks on the system must be via encrypted protocols (e.g., ssh, ssl)
- The system shall provide a mechanism to authenticate a remote user (i.e., verification of network address etc.)
- The system / application administrator shall be able to re-set passwords (e.g. when the actual password is unknown).

Platform and Operating System Setup

- All parts of the system shall be hardened. If specific requirements are not provided by AGRA, the system and its parts shall be hardened at least according to the specification provided by the manufacturer of the product. In this case, the proposed hardening shall be in accordance with AGRA Security standards and shall be agreed by AGRA.
- All unused software packages or those not required for the functioning of the system shall be outlined; applications and services not required shall then be deactivated and/or removed from the system.
- All components used shall be of the latest available version with all security patches / service packs applied.
- An exhaustive list of all the installed security patches and modifications shall be provided.

Accountability and non-repudiation

- Security log files shall be protected against manual modification even by the super user.
- The system must provide for configurable setting of maximum size of audit logs. When the audit log file gets full, it shall either switch to a second file or overwrite itself but only AFTER proper back-up has taken place.
- Access to the logging functionality and system logs data shall be restricted to privileged accounts and user profiles.
- The system shall provide the capability to detect multiple logons from the same user ID, by geography, and restrict users to specified sessions at a time.
- The system must provide for a configurable setting of log retention period and allow for archiving of logs.
- The system shall provide the capability to export audit logs into database, spreadsheet, or word-processing formats.
- A configurable automated process shall be implemented to send log files or defined logged event to a security log server.
- The system shall provide audit trails on different software layers (Operating System, database, application) ensuring a tight control of accessed functions and information.
- All events relevant for security (logins, failed logins, logins while a session is already established, rejected connections, violations of access restrictions, manipulation attempts, fraud etc.) shall be logged with all available information (e.g., time, date, type of event, IP-address, location, etc.). The system should provide the capability to export these logs.

Compliance to Terms of Use

System shall display a notice indicating that only authorized users are allowed access to the system in accordance with any legal/corporate obligations.

Availability and Business Continuity

- The solution vendor must describe how the proposed solution will meet requirements of high availability.

- A Disaster Recovery process shall be documented and tested for the solution.
- A definition of supported back-up plan shall be provided for the system.

3. Deliverables

The following deliverables are expected from the ERM Automation System project:

a. **System Requirements Specification:** A detailed document specifying the functional and technical requirements of the Enterprise Risk Management System.

b. **System Design and Configuration:** The design and configuration of the ERM processes automation System, including data models, workflows, integrations, and user interfaces.

c. **System User Acceptance Testing:** Develop test scripts, plan and execute test strategy.

d. **System Implementation:** The development, testing, and deployment of the ERM processes automation System in the organization's environment i.e., development and configuration of the system, including customization, user interfaces, workflows, data migration, and testing.

e. **Data Migration:** Transfer existing risk-related data from legacy systems or manual records to the new system, ensuring data integrity and accuracy.

f. **User Training and Support:** Conduct training sessions to familiarize users with the system's functionalities, provide user manuals, and establish ongoing support mechanisms.

g. **System Documentation:** Prepare comprehensive system documentation, including system configuration workbooks, user guides, technical manuals, system administration guidelines, and maintenance procedures.

h. **System Maintenance and Support:** Ongoing system maintenance, bug fixes, and user support after the system implementation. Bidders must include in their financial proposal maintenance & support costs covering the 1st three years after post-implementation support.

4. Project Timeline & Resources

The timeline and required resources for the ERM System Automation project will be determined during the planning phase. This will include developing a project charter, defining project timelines, milestones, allocating personnel, and identifying any external expertise or vendors required for successful implementation.

5. Project Governance

The project shall be spearheaded by a **Project Steering Committee (PSC)** for proper governance. The Steering Committee shall consist of proficient managers who have the power/authority to make decisions within their business units. The PSC shall hold accountability and responsibility for the overall success and timely project completion. The committee members shall include stakeholders and relevant organizational resources representative of the organization.

The Project Charter: The roles and responsibilities of each stakeholder and member of the PSC shall be clearly defined in the project charter. The Project Manager will have the critical responsibility of administering efficient use of resources within the defined jurisdiction and ensure proper communication pathways are established with vendors/suppliers or contractors. The Project Manager shall oversee the day-to-day activities of the project on behalf of the PSC, and shall play a key role in the overall project decisions taken.

Vendor and AGRA-side stakeholders shall be specified at project onset and such resources shall remain unchanged for the entire project lifecycle, unless backed by a written approval by AGRA.

6. Required Skills, Competencies and Experience

a. Requirements for the Firm

i. Legally registered organization with staff that have at least 5 years professional experience and knowledge in the implementation, maintenance, and support of the proposed Enterprise Risk Management (ERM) solution.

ii. Provide a support governance structure suitable for the assignment.

iii. Ability to manage work of a confidential nature and handle large volumes of work with short delivery timelines.

iv. Should demonstrate experience in: -

1 Implementing & supporting ERM solutions in a complex business environment and

2 Working with international organizations with distributed work locations.

v. Planning and delivering results under tight deadlines.

vi. Willingness to take ownership of issue analysis and resolution efforts and commitment to “doing what it takes” to resolve technical issues strictly within agreed-upon Service Levels.

b. The Firm must have Product certified support personnel with the following qualifications:

i. The assigned resources must be certified software engineers in the proposed ERM solution, with good communication and excellent expert product knowledge and skills.

ii. They must possess current certifications in the ERM product they implement/support with at least 5 years’ experience providing specialist product implementation & support covering customization, configuration, troubleshooting, and resolving complex issues as well as working with other solutions providers to ensure seamless integrations between the ERM solution and other software solutions.

iii. An advanced degree in Information Technology, Computer Science, Engineering, or any other related fields, with professional certifications in each of the solutions to be implemented and supported.

iv. Hands on experience in troubleshooting, resolving OS and DB-related issues.

v. Previous working experience in a multicultural environment or not-for-profit institution like AGRA would be an asset.

vi. Good command of English, both written and spoken.

vii. Able to work under challenging circumstances with minimum supervision.

viii. The project team leader and the associate team leader should have prerequisite knowledge and good understanding of Enterprise Risk Management & Compliance in a highly digitalized organization.

ix. Have own dedicated team to handle integrations that may be required.

7. Evaluation Criteria

Interested firms shall be evaluated against the following technical criteria:

Evaluation Criteria	Sub criteria/Description	Score
Organization Capacity	Bidder to provide a summary of the firm's profile highlighting • Years of existence • Experience with implementation of systems in similar organization • Firm's organization structure (Management and technical support capacity) • Certifications and/or accreditations • Portfolio of clients	10 points
Firm's Past Experience.	• Firms experience in implementation of ERM systems • Firm must provide at least three reference letters/LPOs/ evidence from clients for having implemented similar systems in the last 4 years (2020-2023)	15 points
Key personnel (Implementation team);	Firms must provide the detailed description of its proposed implementation team providing CVs of at least the below key Personnel 1. Project Manager 2. System Implementation/development Expert 3. Other Key experts Provide CVs and relevant certifications. Qualifications and experience required is highlighted in section 6 above.	20 points
Methodology/ Approach	Bidder must describe its implementation approach, need assessment, system review, etc. Maximum 5 pages	10 points
Implementation work-plan,	Provide a clear timeline and work schedule on the implementation. Provide the complete duration required to do the complete implementation and integration of the system to AGRA's	10 points

	requirement.	
System Technical Conformance (see questionnaire below)	1. Functional requirements 2. Non-functional and technical requirements 3. Enterprise requirements	35 points
Total		**100 points**
Note: • Minimum technical score – 75% • Selection Method – Quality and Cost Based Selection (QCBS) • Weightage: Technical – 80%, Financial – 20%		

System Technical Conformance:

Please use the following matrix as a key for responding to the requirement tables in the RFP.

Response Code	Description	Bidder's response (indicate response code)
E - Existing	Feature is delivered as standard functionality in the proposed version of the software and can be demonstrated by the vendor.	
F - Future	Feature is not currently included but will be available in a future release. Please indicate time frame (e.g., 12 months).	
CC - Customer Customization	Not included. Tools are provided for customization at no additional cost.	
VC - Vendor Customization	Not included. Vendor provides customization at an additional cost.	
TP - Third Party	Feature is provided by a third-party partnering arrangement. Indicate any preferred partner agreements.	
NA - Not Available	Requirement cannot be met.	

a. Functional Requirements

Using the response codes indicated above, respond to each of the requirements below. You may provide a clarification comment if deemed necessary.

#	Requirements	Code	Comments
1	**Risk Identification**: The system should allow for the capture and updates of identified risks across various organizational units, countries, programs, divisions, and departments. It should support the capture of risk events, risk sources, and associated control measures.		
2	**Risk Assessment**: The system should facilitate the assessment of risks based on their impact and likelihood. It should provide a standardized methodology for risk scoring and prioritization.		
3	**Risk Register and Repository**: The system should offer a centralized database to store and manage risk information and classification of risks based on categories, impact, and likelihood, as well as the ability to track risk ownership and accountability.		
4	**Risk Mitigation Planning and Tracking:** Should have workflow capabilities for creating and monitoring risk mitigation plans, assignment of responsibilities, implementation dates, progress tracking and reminders for tasks according to defined trigger points.		
5	**Risk Monitoring:** The system should enable the continuous monitoring of identified risks. It should allow for the tracking of risk mitigation actions, monitoring of key risk indicators, and automatic notifications of critical risk events.		
6	**Reporting and Analytics:** The system should enable generation of comprehensive and customizable risk reports and dashboards. It should provide robust analytics and visualization tools to aid in decision-making.		
7	**Risk Appetite and Tolerance Framework:** The system should enable specification of risk appetite and tolerance levels and monitoring and reporting on risks exceeding defined thresholds.		
8	**Incident and Issue Management:** Offer		

#	Requirements	Code	Comments
	capabilities for escalation mechanisms for significant risks and system for reporting and tracking risk-related incidents and issues through escalation and notification mechanisms and collaboration features for incident resolution.		
9	**Integration:** The system should integrate with existing organizational systems, such as the audit management system, to ensure seamless data exchange and avoid data duplication.		
10	**Security and Access Control:** The system should incorporate robust security measures to protect sensitive risk-related information. It should allow for role-based access control to ensure appropriate access rights for different user groups.		
11	**High Impact Risk Register Log**: Maintain a risk register log for high impact risks across the organization and integrate with the audit management system (teammate+).		

b. Non-Functional Requirements and Technical Requirements

Using the response codes indicated above, respond to each of the requirements below. You may provide a clarification comment if deemed necessary.

#	Requirements	Code	Comments
	Integration and General Requirements		
1	System to support Service Oriented Architecture (SOA)		
2	Provides multi-lingual capabilities, in particular, English, French and Portuguese		
3	Dedicated process management tool that ideally controls processing and sequencing of orders across various systems to facilitate interoperability of applications.		
4	Messaging bus that handles communication between applications to facilitate interoperability of applications.		
5	Reports on failed transactions and recognize transaction failure notification from external systems as communicated by the messaging service bus.		

#	Requirements	Code	Comments
6	The proposed solution must provide comprehensive and easily accessible on-line help facilities to the users.		
7	Provides extensive reporting capabilities, including in-built report generation tools.		
8	Generates information that is compliant with generally accepted protocols/formats and standards, for consumption and use by an external BI and DW tool.		
9	Supports and enforces compliance through a detailed audit trail of every transaction- (user information and transaction history data)		
10	Supports a 24X7 availability.		
11	Can support a modular architecture that corresponds to the business processes in order to support a phased implementation.		
12	Supports fault tolerance.		
13	Integrates with a secure inbound and outbound email messaging platform.		
14	Provides integrated error and exception handling capabilities.		
15	Tracks business rules parameters for different time periods		
16	Permits the "posting" of data transactions in real time.		
17	The system can "roll back" non-committed transactions in the event of a system failure.		
18	Supports centralized process scheduling mechanisms.		
19	Ensures that the failure of any end user devices, e.g., workstations, printers, does not impact the operation or performance of other devices.		
20	Provides failover management capabilities for both application and database server.		
21	Can support a maximum latency of not more than one second for all acknowledgements, and, not more than 5 seconds for final delivery.		
22	Supports the assignment of priority to system functions (search, exports, backup)		
23	Provides validity checks on data elements at the point of data entry.		

#	Requirements	Code	Comments
24	Facilitates rapid data entry for large volume or high-speed data entry requirements.		
25	Allows automatic saving of work in progress.		
26	Allows the user to resume work in progress and also modify previously saved work in progress.		
27	Supports and executes structured workflows and allows the design and customization of workflows (around both processes and transaction types)		
28	Can embed SLAs within process workflows and supports SLA management (for example turn-around time for transactions), monitoring and reporting at individual transaction type level.		
29	The system should be able to work with outbound mail to communicate SLA non-compliance.		
30	Allows for development and customization of data capture/UI forms, including definition of parameters at form object level to enhance integrity of data capture on the various forms.		

c. Enterprise Requirements

Using the response codes indicated above, respond to each of the requirements below. You may provide a clarification comment if deemed necessary.

#	Requirements	Code	Comments
	Security Concept: The security concept shall include:		
1	An explanation of the system architecture, describing how the functional components are distributed / localized in the architecture, the standard platforms (e.g., hardware, OS, middleware, applications, and databases.		
2	Interfaces with other systems/applications and protocols.		
3	All installed & uninstalled components or applications shall be documented in the security concept.		
4	All supplier related Operations and Maintenance Procedures and roles shall be documented in the security concept.		

#	Requirements	Code	Comments
5	All remote maintenance procedures shall be stated in detailed documentation and are subject to ongoing security audits.		
6	All implemented and available authentication and authorization mechanisms shall be documented in detail, whether the features / functions are enabled or disabled, used or unused.		
7	The security mechanisms, available to secure the system against unauthorized use, manipulation, or disclosure of information on all application tiers shall be documented.		
8	An exhaustive list of all the installed security patches and modifications shall be supplied.		
9	The requirements of the system concerning security of the network infrastructure (e.g., firewall ports, DMZ configurations. etc.) shall be documented.		
10	User password requirements (e.g., minimum password length, maximum password lifetime, screen lock timeout, password complexity, maximum number of failed login attempts) shall be documented.		
11	An explanation of the concept used to archive log files in a trustworthy way for a configurable period of time according to resources and requirements shall be documented.		
12	Backup recommendations shall be provided by vendor and validated.		
13	Protocols/services which use random or dynamic network ports or port ranges are not allowed.		
14	The system shall have standards-based interfaces, at both the protocol and data representation levels, in order to facilitate operating within a security framework. All protocols shall be compatible with Firewalls, Network Address Translation and DNS.		
15	Interfaces and Protocols shall provide encryption and authentication based on industry-recognized standards.		

#	Requirements	Code	Comments
16	Ability of the Identity Directory to support authentication of users via Windows AD SSO, SAML tokens or Integrated Security.		
	Security and Integrity		
17	There shall be measures to safeguard against user error and fraud (i.e., system must check the validity of data entered into the system or imported from other applications.		
18	Critical / Confidential data shall not be stored anywhere where it could be at risk and shall be able to be encrypted whilst stored or transmitted (for example, encrypt credit card details stored in a database).		
19	The passwords used or required for the administration and for the operation of the system shall NOT appear in plain text in any file, or database.		
20	The system shall provide a granular access control mechanism that will determine functionality and data which users of various roles can have access to read write and execute. The principle employed should be that of "Least Privilege".		
21	System menu and screen functionality shall be based on a policy where, by default, no one is allowed to access anything, unless explicitly permitted so.		
22	All passwords shall be stored hashed or in a one-way encrypted form that is inaccessible by all users. They shall not be written in any file or database (i.e., log or cookie, cache, etc.).		
23	End User (including customer) passwords shall be inaccessible by any kind of user.		
24	Administrators will only be able to reset a user's password but not be able to see a user's password.		
25	The system must not have any hard-coded passwords (i.e., service/application user passwords displayed in source code)		

#	Requirements	Code	Comments
26	End users shall be able to change their own passwords (provided the previous password is known) without requiring intervention of system administrators.		
27	The system shall enforce strength of passwords. System must provide a configurable mechanism to detect and block simple passwords.		
28	The system shall provide the capability to lock/deactivate/suspend or delete certain accounts/user IDs either manually or automatically, given some predefined actions/criteria (e.g., period of inactivity, defined number of failed logins attempts etc).		
29	The system shall provide the capability to extract and print a list of all possible access privileges.		
30	The system shall provide the capability to extract and print a specific user's access privileges.		
31	All users shall be allocated a unique user ID for the sole use of the individual. The system must not have functionality that requires generic user accounts.		
32	The number of unsuccessful log-on attempts shall be limited to a configurable number of attempts per session; afterwards, the session will be terminated.		
33	Remote operation and maintenance tasks on the system must be via encrypted protocols (e.g., ssh, ssl)		
34	The system shall provide a mechanism to authenticate a remote user (i.e., verification of network address etc.)		
35	The system / application administrator shall be able to re-set passwords (e.g. when the actual password is unknown).		
	Platform and Operating System Setup		
36	All parts of the system shall be hardened. If specific requirements are not provided by AGRA, the system and its parts shall be hardened at least according to the specification provided by the manufacturer of the product. In this case, the proposed hardening shall be		

#	Requirements	Code	Comments
	in accordance with AGRA Security standards and shall be agreed by AGRA.		
37	All unused software packages or those not required for the functioning of the system shall be outlined; applications and services not required shall then be deactivated and/or removed from the system.		
38	All components used shall be of the latest available version with all security patches / service packs applied.		
39	An exhaustive list of all the installed security patches and modifications shall be provided.		
	Accountability and non-repudiation		
40	Security log files shall be protected against manual modification even by the super user.		
41	The system must provide for configurable setting of maximum size of audit logs. When the audit log file gets full, it shall either switch to a second file or overwrite itself but only AFTER proper back-up has taken place.		
42	Access to the logging functionality and system logs data shall be restricted to privileged accounts and user profiles.		
43	The system shall provide the capability to detect multiple logons from the same user ID, by geography, and restrict users to specified sessions at a time.		
44	The system must provide for a configurable setting of log retention period and allow for archiving of logs.		
45	The system shall provide the capability to export audit logs into database, spreadsheet, or word-processing formats.		
46	A configurable automated process shall be implemented to send log files or defined logged event to a security log server.		
47	The system shall provide audit trails on different software layers (Operating System, database,		

#	Requirements	Code	Comments
	application) ensuring a tight control of accessed functions and information.		
48	All events relevant for security (logins, failed logins, logins while a session is already established, rejected connections, violations of access restrictions, manipulation attempts, fraud etc.) shall be logged with all available information (e.g., time, date, type of event, IP-address, location, etc.). The system should provide the capability to export these logs.		

8. Application Submission Requirements

a. Technical proposal

i. Company profile

ii. Proposed Methodology and implementation plan.

iii. Detailed reference list indicating the scope and magnitude of similar assignments carried out.

iv. Duly filled questionnaire on conformance to system technical requirements.

v. Proposed key staff, their roles including their CVs, academic and professional certificates.

vi. The technical proposal shall not exceed 15 pages. CVs, copies of academic and professional certificates and other supporting documentation may be attached as annexes.

vii. Firms may be required to make presentations on their proposal/proposed solution.

b. Financial Proposal

a. The firm shall indicate on oracle (under ‘’Lines’’ section) the total annual applicable fees for carrying out the assignment. These shall include the sum of professional fees, reimbursements if applicable, and applicable Kenyan taxes. A VAT of 16% will apply to firms registered in Kenya. For firms not registered in Kenya, the applicable WHT tax will apply.

b. The detailed financial proposal shall be attached on the system and should include the professional fees per consultant, reimbursables, maintenance & support costs covering the 1st three years after post-implementation support and applicable taxes.

c. Reimbursable expenses will be reimbursed based on actual cost incurred and upon submission of receipts.

d. If the financial proposal is silent on taxes, AGRA shall assume that these are inclusive.

e. Prices must be quoted in USD ($) or Kenyan Shillings.

f. Please note that the oracle system will seal the financial proposals until the technical evaluation is completed. Financial proposals will not be opened until the conclusion of the technical evaluation and then only for those proposals that meet the minimum technical score of 75%.

9. Guidelines For Preparations and Submission of Proposals

a. The Proposals shall be prepared in English Language.

b. The proposals SHALL be submitted via oracle system by the deadline indicated in the system.

c. The technical proposal shall not exceed 15 pages. CVs, certificates, and other supporting documents should be added under annexes.

d. The proposal and ALL Attachments submitted via oracle system SHALL NOT exceed 10MB.

e. VALIDITY of the proposal shall be for a period of 90 days from the date of bid closure.

f. The detailed financial proposal shall be sent as a separate attachment.