Department for International Development

UKaid from the British people

Section 4 Appendix A

CALLDOWN CONTRACT

Framework Agreement with:	**AECOM Ltd**
Framework Agreement for:	**DFID Goods & Equipment Procurement Supplier**
Framework Agreement Purchase Order Number:	**7387**
Call-down Contract For:	**Procurement of an Automatic Exchange Software for Ghana Revenue Authority (GRA)**
Contract Purchase Order Number:	**PO 8517**

I refer to the following:

1. The above mentioned Framework Agreement dated 29th March 2016

2. Your proposal of 10th April 2019

and I confirm that DFID requires you to provide the Services (Annex A), under the Terms and Conditions of the Framework Agreement which shall apply to this Call-down Contract as if expressly incorporated herein.

1. Commencement and Duration of the Services

1.1 The Supplier shall start the Services no later than 3rd June 2019 ("the Start Date") and the Services shall be completed by 30th September 2019 ("the End Date") unless the Call-down Contract is terminated earlier in accordance with the Terms and Conditions of the Framework Agreement.

2. Recipient

2.1 DFID requires the Supplier to provide the Services to the **Ghana Revenue Authority (GRA)** ("the Recipient").

3. Financial Limit

3.1 Payments under this Call-down Contract shall not, exceed £**989,009.22** ("the Financial Limit") and is exclusive of any government tax, if applicable as detailed in Annex B**.**

4. DFID Officials

4.1 The Project Officer is:

REDACTED

4.2 The Contract Officer is:

REDACTED

5. Reports

5.1 The Supplier shall submit project reports in accordance with the Terms of Reference/Scope of Work at Annex A.

6. Duty of Care

All Supplier Personnel (as defined in Section 2 of the Agreement) engaged under this Call-down Contract will come under the duty of care of the Supplier:

I. The Supplier will be responsible for all security arrangements and Her Majesty's Government accepts no responsibility for the health, safety and security of individuals or property whilst travelling.

II. The Supplier will be responsible for taking out insurance in respect of death or personal injury, damage to or loss of property, and will indemnify and keep indemnified DFID in respect of:

II.1. Any loss, damage or claim, howsoever arising out of, or relating to negligence by the Supplier, the Supplier's Personnel, or by any person employed or otherwise engaged by the Supplier, in connection with the performance of the Call-down Contract;

II.2. Any claim, howsoever arising, by the Supplier's Personnel or any person employed or otherwise engaged by the Supplier, in connection with their performance under this Call-down Contract.

III. The Supplier will ensure that such insurance arrangements as are made in respect of the Supplier's Personnel, or any person employed or otherwise engaged by the Supplier are reasonable and prudent in all circumstances, including in respect of death, injury or disablement, and emergency medical expenses.

IV. The costs of any insurance specifically taken out by the Supplier to support the performance of this Call-down Contract in relation to Duty of Care may be included as part of the management costs of the project, and must be separately identified in all financial reporting relating to the project.

V. Where DFID is providing any specific security arrangements for Suppliers in relation to the Call-down Contract, these will be detailed in the Terms of Reference.

7. Call-down Contract Signature

7.1 If the original Form of Call-down Contract is not returned to the Contract Officer (as identified at clause 4 above) duly completed, signed and dated on behalf of the Supplier within 15 working days of the date of signature on behalf of DFID, DFID will be entitled, at its sole discretion, to declare this Call-down Contract void.

For and on behalf of The Secretary of State for International Development	Name: Position: Signature: Date:
For and on behalf of AECOM Ltd	Name: Position :

Department for International Development

UKaid from the British people

Signature :

Date :

Department for International Development

UKaid from the British people

Table of Annexes per Calldown Contract

Annex	Description
Annex A	Terms of Reference
Annex B	Specifications
Annex C	Procurement Plan
Annex D	Schedule of Prices
Annex E	KPIs and SLAs
Annex F	Savings management
Annex G	Communication Matrix
Annex H	Duty of Care country assessment

Department for International Development

UKaid from the British people

Annex A

Ghana Revenue Reform Programme (GRRP)
Terms of Reference for Procurement of an Automatic Exchange Software for Ghana Revenue Authority (GRA)

1.Context

The UK Government through its Department for International Development (DFID) is providing funds over a period of four years (2015 to 2019) to support the Ghana Revenue Authority (GRA) and Ministry of Finance in Ghana to strengthen sustainable system for domestic revenue generation. The intervention supports a combination of tax policy and administrative reforms to improve domestic revenues and to address immediate macro consolidation issues.

As part of our interventions we are providing financial assistance to GRA to acquire a robust and secure software to enable it participate in the data exchange with other approved international authorities through the Automatic Exchange of Information Act.

It has proven essential to strengthen GRA's capacity to curb the issue of international tax evasion and avoidance. The parliament of Ghana passed a Law, the Standard for Automatic Exchange of Financial Account Information Act, 2018 (Act 967) in May 2018. The act covers exchange of information . exchange of information on request, spontaneous, and on an automatic basis of banking and other details amongst the Parties.

2.Objectives

GRA needs to acquire recognized CRS compliant software, which would be effective, cost friendly and also has the features which are compatible with other member jurisdictions. Procurement of the software is a basic requirement if Ghana has to fulfill its international obligations of tax transparency and sharing of information with other countries.

Hence, the major objectives of this proposal are:

i. To provide GRA with a framework to report information on financial accounts to the respective participating jurisdictions under CRS, as obtained from the reporting financial institutions in Ghana under the Common Reporting Standard (see http://www.oecd.org/tax/automatic-exchange/common-reporting-standard/ for more details).

ii. To provide the interface (the "Portal"), between GRA and industry which enables the secure and efficient reporting of the required tax information under CRS. GRA envisages that this information-technology solution will be developed from a pre-existing platform provided by a supplier of a proven and previously deployed CRS IT system with successful implementation in other jurisdictions which will be adapted to meet the requirements of the Project.

iii. To provide support for GRA in the form of helpdesk that shall be run by the Portal vendor during business hours (i.e. 9am - 5pm) for 2 years to commence after the successful commissioning and deployment of the complete software/portal.

3. Recipient

The proposed project is to be deployed within a secure perimeter in the Ghana Revenue Authority Head Office in Accra. The selected supplier will be assigned staff from the GRA in all movements in the GRA. The recipient is thus the GRA and the DFID Ghana, the funding entity.

4.Scope

AECOM will develop and agree a procurement schedule with GRA and DFID Ghana including finalising the specifications and amounts to be tendered and agreeing the sequence of procurement of the software**.**
AECOM will undertake the procurement of the software in a timely and accountable manner, in accordance with the terms and conditions and scope of services of DFID framework (AECOM) and taking into account Whole Life Costing (WLC). Once the software arrives in Ghana, AECOM and their supplier will collaborate with the GRA IT team in its deployments.

a) Supply, configure, adapt and customize for GRA a Common Reporting Standard (CRS) - compliant software and provide the required hardware. GRA will provide the secure environment for the implementation of the software.
b) Be responsible for the complete deployment along with the training to the users.
c) Arrange for a helpdesk for ongoing support for a period of two years after the successful commissioning and deployment of the complete software.

The proposed software should fully be an automated web solution that allows users to upload the information with regard to the reporting regimes outlined above and GRA to directly forward that information to the respective foreign tax authorities, to the extent reasonably and practicably possible.

The technical specifications and the functional requirements for CRS Compliant Software are detailed at **Appendix 1**

5.Method

In accordance to the Overarching Framework Agreement PO 7387, response times for key procurement activities against which AECOM's performance shall be measured as detailed in Annex E.
Timing and procurement planning are critical to the successful implementation of the project. AECOM will be expected to demonstrate efficiency, effectiveness, accountability and transparency, and measure and record its associated value added. Annex C denotes the Procurement Plan.
Clear communication channels and / or approval process will be established between AECOM and DFID Ghana at the onset of contract. Annex G denotes the Communication Matrix.
DFID Ghana Commercial Adviser and DFID Ghana Programme Manager will be kept informed by AECOM of all relevant issues likely to affect the implementation of the Programme.

6.Outputs / Deliverables

The Procurement Supplier (AECOM) of DFID Ghana will:

- Review the Terms of Reference and technical specification and suggest changes that may be required before approaching the market.
- Undertake all sourcing as per the terms and conditions of any agreement entered into with DFID.
- Procure the software in line with the objectives of the CRS and Automatic exchange of Information, liaising with GRA throughout the process.
- Negotiate after sales/installation in-country support by the equipment manufacturers and software providers with the aim of ensuring continuing full operation of proposed solution and building of local capacity to manage the system.
- Agree with the manufacturer to install, provide training to approximately 15 GRA staff operating from the secure perimeter, maintain and/or troubleshoot and also have a service representative/helpdesk available. The duration and timing of the GRA Staff Training is to be proposed by the Supplier.
- Ensure that the operating manuals/audio/visual CDs and the requisite software of the products are available to GRA and reference for trained users
- Ensure that the equipment and software is of required specifications and conforms to the quality standards outlined in the Technical Specification.
- Manage the supply base in relation to quality, cost and delivery time. The Procurement Supplier (AECOM) will ensure supply of equipment and software and delivery to the GRA assigned secured perimeter at its Headquarters in Accra. Installation of the equipment and software, and training of GRA staff on operation, maintenance and troubleshooting will be covered in the service agreement by the Supplier.
- The procurement Supplier will provide a procurement plan with key milestones and provide regular progress reports on ongoing achievement of these milestones. These reports shall be submitted to DFID Ghana and GRA.
- Maintain close coordination with GRA on technical requirements and ongoing training requirements. Undertake thorough due diligence and capacity assessment of the manufacturers before awarding contract.

The Supplier will:

- Install and deploy a CRS compliant software according to the technical specifications and the Functional requirements for CRS Compliant Software
- Install, provide training to GRA staff, maintain and/or troubleshoot and also have a service representative/helpdesk available for 2 years after commissioning and deployment of the complete software/portal. Training on software usage can be accomplished within 2 weeks at a max. However, training on support may vary based on the complexity of the software solution selected. Also, the server (acquired separately by WB) may be access remotely via a secure connection for system troubleshooting and support by vendors.
- Provide reports according to the reporting section below
- Provide training according to the training requirements in the Technical Specification
- Develop an effective risk plan

7. Reporting

AECOM will report to the DFID nominated personnel. The reporting chain may be changed at DFID's discretion due to reallocation of responsibilities within DFID. AECOM will be required to deliver the following mandatory outputs:

a) Within 3 months of completion of the project, or at a time agreed with DFID, a project completion report in DFID standard format.
b) A final report will be submitted to DFID Ghana by the Procurement Supplier (AECOM) providing details of deliverables achieved during the procurement period.
c) Provide report and summaries of progress against work plan deliverables and outputs.
d) A final report will be submitted to DFID Ghana by GRA providing details of deliverables achieved during the procurement period.

8. Timeframe

The Supplier will be contracted for the period between the start date and the end date as stated on page 1 of this contract, any extension to the end date will need to be agreed by both parties by contract amendment.

9. DFID Co-ordination

AECOM will report to DFID Ghana Procurement Officer and DFID Ghana Programme Manager. The Communication Matrix is attached as Annex C.

10. Payment

Payments will be linked to the delivery of the requirement. AECOM's fees will be a percentage of the value of the procured goods and equipment, as detailed in the Procurement Plan attached at Annex F.

AECOM will be required to maintain a record of any relevant expenditure incurred in the programme activities and keep original copies for the record for the entire duration of the programme.

An inventory of all assets procured under the programme will be maintained by AECOM. At the end of the programme period or once the contract has been completed, DFID Ghana will decide in consultation with key stakeholders how best to dispose of assets acquired with DFID Ghana funding.

AECOM will liaise with DFID Ghana to ensure that all relevant documentation pertaining to any exemptions from tax that may apply to the procurement are obtained.

11. Duty of Care Country Assessment

Country: Ghana
Date of Assessment: February 2018
Assessing official: DFID Ghana Corporate Effectiveness (CORE) Team

Theme	DFID Risk score
	Other parts of Ghana

OVERALL RATING[1]	2
FCO travel advice	2
Host nation travel advice	FCO Travel Advice
Transportation	2
Security	2
Civil unrest	1
Violence/crime	2
Espionage	1
Terrorism	1
War	1
Hurricane	1
Earthquake	1
Flood	2
Medical Services	2
Nature of Project/Intervention	

1 Very Low risk	2 Low risk	3 Med risk	4 **High risk**	5 Very High risk
Low		**Medium**	**High Risk**	

Supplier to confirm with DFID Ghana Programme Team that the above Assessment has not been subsequently updated when finalising their own Risk Assessment. The ratings have been provided by DFID Ghana Security Section but with the proviso that these are generic to the country as a whole, and Suppliers may apply local knowledge or experience to amend these in their own risk assessments, or to take into account local variations. DFID Ghana Duty of Care Assessments are updated roughly annually, or in response to an event.

Contact Names:
Ama Blankson-Anaman Economic Adviser DFID Ghana
Kosua Oheneba-Gyambibi Business Support Manager DPO DFID Ghana

Appendix 1
Supplier and general requirements:

1. The proposed solution must be provided by a supplier of a proven and previously successfully deployed CRS IT system.
2. The proposed solution must include all necessary software, training, secure

[1] The Overall Risk rating is calculated using the MODE function which determines the most frequently occurring value.

implementation, warranty and support components required to deliver a turn-key solution.

Functional requirements for CRS Compliant Software:

i. The proposed solution must provide the following functionality:

a) The capability for financial institutions to self-register and create and manage an account in accordance with the requirements of the CRS.

b) Monitoring and approval workflow to provide oversight and management to GRA of the registration process undertaken by financial institutions.

c) Support for the electronic reporting of data by financial institutions to GRA as prescribed by the CRS, and domestic legislation, in accordance with the published applicable Extensible Markup Language ("XML") schema to include all applicable data validation.

d) Support for the option to complete manual data entry of returns directly into the Portal interface using a Web Form, or similar, by those financial institutions not wishing to submit an XML file and conversion of the manual entry into the required schema(s) for onward submission of that information by GRA to the respective tax authorities.

e) Support for requests for information made under Tax Information Exchange Agreements ("TIEAs") by partner jurisdictions where automatic exchange of information is not yet in place or is not in use, to include full case management, history, associated document management and management reporting.

f) Secure, automatic (as appropriate) electronic transmission of reported data cross-border to CRS partner jurisdictions, in accordance with relevant business rules and technical schemas, and the IRS international data exchange service ("IDES").

g) Support for changes made to the applicable CRS schemas as may occur from time-to-time to ensure that necessary updates are applied to the Portal in a timely manner in accordance with the instructions issued by the applicable authority without additional cost to GRA. The requirement is to have an Admin interface for GRA where the minor configuration changes required can be carried out without the supplier's intervention whereas for any major change/upgrade such as; addition of an interface will be carried out by the supplier, with an agreed Change Request Procedure, during the support and maintenance period.

h) Support for sufficient scalable capabilities to ensure a comprehensive and integrated approach in accommodating reporting and transmission requirements for multiple partner jurisdictions is delivered to enable GRA to remain in compliance with the obligations identified in the CRS and CbC. Scalability would be considered by keeping in mind the strength of the current Financial Institutions and capability of the system for future growth.

i) Support for sufficient capacity in design to accommodate up to 5,000 reporting financial institutions, including the ability to handle multiple submissions and multiple users. Considering the expected five year future growth GRA have estimated the number of reporting financial institutions to 5,000. These include banks, leasing companies, brokerage houses and investment banks etc.

j) Support for the automated exchange of information with other jurisdictions as they are added to the CRS and CbC population of reporting countries in order to ensure that GRA remains in compliance with its obligations.

k) Compliance with the technical specifications in accordance with published CRS and

CbC schemas and Implementation Packages, including (but not limited to) requirements for certificate / access management, encryption, exchange services, identification and authentication, audit and accountability, business rules and user delivery notification.

l) The application MUST adhere to all security requirements of CRS& TIEA and it should also comply with the security standards of CbC / TIEA.

m) Adherence to Open Web Application Security Project ("OWASP") testing protocols which will be conducted as a test case as part of the solution acceptance criteria.

n) Support for downloading security patches and product updates. The Portal should have a mechanism in place to alert users about such updates/patches. The Procurement Supplier should also describe the procedures for applying software updates and upgrades. The updates for the portal will be manually after accessing the impact of these updates in a test environment. However the guidelines for the updates have to be shared by the supplier. The requirement for the patches update is manual in order to maintain the integrity of the system. GRA are insisting on manual as an integrity check prior to its implementation in production.

o) Support for responsive access via modern browsers including Internet Explorer, Chrome, Firefox, and Safari. This support must not be bound to a particular version or browser.

p) Provision of end-user help in the form of an up-to date user guide available within the Portal to users and ongoing maintenance of associated Frequently Asked Questions. GRA do not have a specific requirement for a tailor made end-user help material however, the user manual should contain screen by screen procedure and process description.

q) Provision of a comprehensive set of management reports and flexible reporting options in order to ensure that GRA had adequate review, tracking and monitoring of information throughout each phase and milestone of the reporting workflow processes related to CRS, TIEA exchange requests. Comprehensive set of reports should include informational reports, analytical reports and customizable reports generated based upon the parameters available within the Dataset.

r) The Procurement Supplier must provide help desk support to end-users of the Portal to assist in the registration and reporting process for 3 years following the successful commissioning and deployment of the complete software/portal.

ii) The Procurement Supplier must specify any physical, environmental or power requirements that represent dependencies for the proposed solution.

iii) The Procurement Supplier must describe in detail the proposed solution management and security solution, as well as any specialized management software that is included or embedded with the hardware/software solution proposed. The management solution must support strong security features including, but not limited to, password attribute customization, authentication logging, role-based access, audit logs and multilevel authorization access. The Procurement Supplier should describe any optional management tools it recommends to specifically enhance operations and the ability to manage the proposed Portal solution.

iv) The Procurement Supplier must define major and minor alarm conditions for the Portal solution, as to how the system responds to each circumstance and describe the capabilities for remote monitoring and automatically reporting fault conditions, both to GRA and supplier personnel.

v) The Procurement Supplier must describe in detail the Service Level Agreement(s) applicable to all components of the Portal solution.

vi) The Portal should provide support for a common format return (e.g. Excel, Access) option, with associated data validation, xml schema conversion and submission.

Mandatory Requirements for CRS Software

i. The vendor must supply proof of external certification of the proposed portal solution, or portal solution components to industry standard security criteria.

ii. The solution must provide support for end-user access to the current applicable CRS Regulations and applicable Guidance Notes within the Portal solution and the ability for GRA to update this content.

iii. The solution must support validation of reported data to ensure data complies with schema requirements of CRS and domestic legislation.

iv. The solution must support automatic electronic transmission of reported data to CRS partner jurisdictions through OECD Common Transmission System (CTS) in accordance with relevant technical schemas. Additional details can be found on the OECD website.

v. The solution must exhibit scalable capabilities to ensure a comprehensive and integrated approach in accommodating reporting and transmission requirements for multiple partner jurisdictions. This refers to the requirement for Automatic Exchange of Information and the countries that have committed to the exchange of information under the Multilateral Competent Authority Agreement. Currently there are 101 countries and jurisdictions which have committed to 2017 or 2018 for the automatic exchange of information. However, this number is bound to increase as more jurisdictions will be joining the Multilateral Convention and committing to AEOI. The procurement Supplier should include an estimate for increasing the number of users linking into the Portal after its successful completion eg the cost of adding each extra user account.

vi. The solution must support reciprocal or non-reciprocal cross-border data transmissions.

vii. The solution must support scheduled bulk transfer methods of data transmission.

viii. The solution must comply to technical specifications of CRS.

ix. The solution must be designed to handle multiple submissions and multiple users

x. The solution must provide support for mobile (smartphone and tablet) devices and browsers, including those on iPhone/iPad and Android devices.

Security

i. The proposed solution must include, at a minimum, password requirements with configurable parameters, access authorization levels, authentication, secure access, logging activities, backup/restore and patching/update capabilities.

ii. The Procurement Supplier must confirm compliance and describe the security features of the proposed Portal solution as requested below:

a. Support for strong (two-factor) authentication, authentication logging, auditing

accounting etc.

b. Administrative user access levels to restrict administration access and flexible password configuration parameters (e.g., password length, aging, complexity).

c. How protection from unauthorized access is achieved

Integration with existing Systems

The Portal part of the CRS solution should be implemented using common web technologies, allowing it to be linked or integrated with the current GRA Portal (from end-user's perspective). The integration will be implemented by GRA using common web technologies. The CRS solution Portal solution should, however, allow this to be done. GRA will make available a link on its public website to point to the CRS Portal or alternatively provide the Portal Link directly to the relevant FIs.

The Solution Supplier is not required to provide support in possible integration of proposed solution with any other existing IT/business systems at GRA.

The possible integration/interworking with existing IT systems is required to be taking place on the level of data-interworking. The proposed solution must be complemented with well documented data import/export procedures relying on clear and widely available data and document formats and languages such as Excel, CSV, XML, SQL.

Warranty and Maintenance for CSR Software

The duration of the validity of the software once installed is preferably a 5-year license for the software, along with 3 years of post-completion support & maintenance services which ensures that the application is kept up to date with changes to the CRS standards and protocols. In year 6 the software would need to be licensed again, but at that time the licensing can be done on a year by year basis.

Additionally, the Procurement Supplier is also required to setup a helpdesk/ticketing system for 2 years for support and maintenance. It can be virtual or in-country from 9am – 5pm work days minus public holidays.

For other software which includes (Operating System, Database Application & Antivirus etc.) GRA requires 3 years comprehensive onsite warranty & support.

Training for CSR Software

For training, the selected Procurement Supplier will be required to provide training to an estimated 15 GRA users and system management communities. Training must include, at a minimum, the administration, management and troubleshooting of the proposed portal solution. Procurement Supplier should describe the training that is recommended in order to use the proposed solution and services. Trainers must have English as a first language. A detailed training schedule should be provided. The schedule should denote class sizes and length of a typical training session. The Procurement Supplier shall also provide pricing for alternative modes of training delivery, if available.

Application & System Software

a) **Database Software**

Oracle/SQL Server as per the requirement in the proposed solution.

This software will be will be required for the configuration of database servers.

b) **SIEM Software**

Designed to collect security log events from numerous hosts within an enterprise and store their relevant data centrally.

Objective of SIEM Solution:

An advanced analytical SIEM solution to provide high-performance advanced threat detection, near-real-time event processing and correlation, historical data analysis, and the integration of contextual and threat intelligence data. This component also must include compliance and incident reporting, automated alerting of common security events, historical analysis for detected incidents and interoperate with other information security systems using industry standard protocols.

The Solution is expected to:

1. Automate the data collection, normalization, correlation, transformation and analysis functions to establish security baselines
2. Identify potential information security issues that are too complex and may not be visible to human eye.
3. Interoperate with other information security systems to participate in the mitigation of identified issues by automating actions based on gathered intelligence to improve the information security posture of GRA.
4. Able to ingest multiple user identity data stores (Active Directory, application database accounts, non-Windows based account, etc.) into the SIEM, have it correlated, analysed and use it to discover end user usage patterns that can be further used to identify anomalies.

SIEM Solution Requirements:

The proposed SIEM solution will collect data from network equipment, applications servers, database servers, application, file and print servers, AD domain controllers, DHCP Servers, etc.

The proposed solution should be secure, high performance, scalable to handle required current and future workloads and be resilient for hardware and network related failures.

The proposed solution must meet the following **mandatory** requirements:

a) Collect, parse, normalize, categorize, and store data from wide variety of systems (i.e. servers, applications, network infrastructure, web based application, etc.)

b) Must be able to sift through, analyze, operate, report on data without creating performance, capacity or response related issues.

c) Correlate and analyze data; detect cyber threats in as close to real-time as possible

d) The proposed design is expected to prevent possible single points of failure within the system. Provide redundancy without being cost prohibitive.

e) Able to assist in performing forensic analysis to determine the root cause of the operational problems and security incidents.

f) Provide security analytics to assist in the analysis of the impact and/or scope of a potential information security incident

g) Expose relationships between physical and virtual machines, network infrastructure, business processes and data, and present the risks and threats in context to provide real-time threat intelligence

h) Provide flexible and resilient deployment options for scalable and non-service or performance impacting log collection

i) Accelerate the discovery and qualification of information security threats

j) Provide daily monitoring (Mon- Fri 9am – 5pm) and participate in automated intelligent response

k) Streamline audits and compliance reporting processes

l) Being able to detect external attacks, data exfiltration attempts and internal misuse in their tracks and interoperate with other information security components to stop these threats

m) The proposed SIEM solution must support industry standard threat information exchange languages/protocols such as “Structured Threat Information eXpression” (STIX) and

"Trusted Automated Exchange of Indicator Information" (TAXII) in order to rapidly add and configure diverse threat intelligence from commercial or open-source feeds

n) Provide operational insight for optimization of information security related workflows

o) Increase information security operational efficiency and expedite incident management processes

p) Provide granular, role-based dashboards (security trimmed) and automated daily reports for authorized staff to review the findings and confirm the integrity of the systems that they are responsible for. Additionally, provide overall system health information to all members of the information security team regardless of their role in the operation of the proposed solution.

q) Provide operational insight for optimization of information security related workflows

r) Increase information security operational efficiency and expedite incident management processes

s) Must produce useful information and spit-out actionable data in a reasonable amount of time in order for GRA to make informed decisions

t) Provide capability to perform root cause analysis of information security related events in real-time with built-in intelligence

u) Provide role-based access security to the system's components, findings and analytics for the GRA's IT Security team to make sure that only authorized staff will have access to the collected information

v) Maintain a detailed logging functionality for the proposed system to retain all system communications, system and user activities, and other critical system information that is pertinent for secure system operations

w) Provide ample growth capacity for compute and storage to add more systems to monitor and collect data from

x) Retain the collected actionable data for at least 12 months

y) Must provide adequate redundancy for hardware

z) The vendor is solely responsible for delivering a fully functional software to match the hardware to be provided by GRA

SIEM Desired Features:

a) Provide capabilities for real-time monitoring, user behaviour baselining, data and user monitoring, application monitoring for threat management and compliance

b) Provide advanced contextual-security analytics utilizing user and entity behaviour analytics (UEBA) and external threat intelligence.

c) Capability to collect logs and other pertinent system information from the monitored systems without installing agent on source systems

d) Provide capability to baseline information security patterns; detect and differentiate between activity patterns that can be good indicators of normal as well as abnormal activity.

e) Able to log data analysis is intended, in part, to help you differentiate between normal and abnormal behaviour.

f) Provide high availability and resilience

SIEM Security and Audit

As a principle, the proposed solution should not cause any security vulnerability to GRA systems.

a) Vendor must provide information about their responsible disclosure program/process.

b) Vendor should provide procedures for patching of the proposed solution including the third party components that the proposed solution relies on.

c) List all third-party software that is necessary for the operation of the solution and will require down time of the proposed SIEM solution during patching.

SIEM Training and Support

Provide manufacturer certified training for 5 employees to be trained to configure, operate and maintain the proposed solutions. Provide a list of digital documents for installation, operation, use, and administration of the whole solution. These documents must be structured, editable, portable, and searchable. All major sections of the content of these documents must be identified within the beginning of each document.

In addition to vendor's official product support, if it is available, the vendor is expected to provide full access to its online forums/user community for the identified staff to get support from their peers from other institutions. In addition to formal classroom training, GRA requires the vendor to provide on-site training of key concepts which are specific to the proposed solution. The vendor must specify the type of training provided. Specify and describe any help files provided by the system. The support is required 24x7 and the Procurement Supplier is required to quote the complete solution with 3 year support and maintenance including the hardware proposed with the solution. The Procurement Supplier is also required to quote the 4th and 5th year recurrent cost separately.

SIEM Implementation

It is desired that the solution architecture is designed to accommodate future growth. GRA expects the selected vendor to provide industry best practices to GRA's staff for the ongoing management of proposed system and any specifics related to the operation of the proposed solution. The following requirements are mandatory:

a) Describe how the solution works during link and device failure.
b) Vendors are required to submit a complete project plan with details and action steps clearly specifying execution items.
c) The vendor is required to provide product road map and its end of life details.
d) The vendor must provide a physical and logical network diagram using Visio tool
e) The proposed design is expected to prevent possible single points of failure within the system.
f) Configure the management tool to provide alerts for failures via phone, text messaging, email etc.
g) Describe how the system logs errors, what error data constituents are documented and how to view useable information from log errors.
h) Describe any monitoring tools or plug-ins that exist to monitor the system.
i) Describe how the system monitors status.

Department for International Development

UKaid from the British people

REDACTED

Annex A	Terms of Reference
Annex B	Specifications
Annex C	Procurement Plan
Annex D	Schedule of Prices
Annex E	KPIs and SLAs
Annex F	Savings management
Annex G	Communication Matrix
Annex H	Duty of Care country assessment


Department
for International
Development


UKaid
from the British people