REQUEST FOR PROPOSAL

IT Security Operations Center-as-a-Service (SOCaaS)

Release Date: **Thursday February 27, 2020**

Last Date for Receipt of bids: Thursday March 19, 2020, 3.00 PM (GMT+3)

Table of Contents

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER

This form is to be completed on receipt of the tender document from Holdings Plc (Britam).

This page is to be completed immediately and scan copy in PDF format e-mailed to procurement@britam.com. The data contained in this form will be used to send out any addenda that may arise. Firms that do not register their interest by completing this form may not be sent addenda that may arise.

Name of the firm's representative completing this form:

_____

Firm's Name: _____

Address: _____

Tel No: _____

Email Address: _____

Signature: _____Date: _____

Signed by (Name): _____

Position in Firm: _____

1 INTRODUCTION

1.0 Purpose of the Tender

The Britam Holdings Plc ("Britam") invites qualified firms to submit their proposals for the Provision of an IT Security Operations Center-as-a-Service (SOCaaS).

This Request for Proposal (RFP) is being made available to interested service providers on a restricted tender basis. This document is intended to provide vendors with sufficient understanding of the Britam's requirements to enable them to respond.

For the purposes of the RFP it is necessary to disclose information in this document, and its schedules, which is considered confidential and should therefore not be used (otherwise other than in furtherance of this tender) or disclosed to any third party without explicit prior written consent of Britam.

Britam on its part also acknowledges that it is requesting through this RFP for information that is confidential and therefore commits in equal terms to reciprocal confidentiality.

1.1 Acknowledgement of Bidding Documents

Britam invites proposals for Provision of an IT Security Operations Center-as-a-Service in accordance with the requirements set out in this document. Within four (4) working days of receipt of the RFP, the Bidder is required to acknowledge receipt of the RFP, and notify his intention to submit a bid by email to Britam at procurement@britam.com. The mail will include the signed registration template on Page 4 of this document.

Working days are defined as being any day of the week between Monday and Friday (0800 – 1700 Hrs) excluding weekends and gazetted public holidays in the Republic of Kenya).

Failure to do so shall be perceived as an intention not to submit a bid and the Bidder will be eliminated from the bid process, and required to destroy the RFP document in keeping with confidentiality requirements.

1.2 Point of Contact

All enquiries or correspondence concerning the details of this tender should be addressed, in the first instance by e-mail to: procurement@britam.com. The subject on the email should be "CLARIFICATION ON THE RFP FOR PROVISION OF AN IT SECURITY OPERATIONS CENTER-as-a-Service (SOCaaS)".

- All responses from Britam to the Bidder shall be channelled through the Procurement Manager.
- It is the responsibility of the Bidder to obtain any further information required to complete this RFP.
- Any clarification request and their associated response will be circulated to all Bidders.
- All clarifications must be sought at the latest 3 days prior to the close of the RFP.

2 ABOUT BRITAM

2.0 Organization Profile

Britam is a leading diversified financial services group, listed on the Nairobi Securities Exchange. The group has interests across the Eastern and Southern Africa region, with operations in Kenya, Uganda, Tanzania, Rwanda, South Sudan, Mozambique and Malawi. The group offers a wide range of financial products and services in Insurance, Asset management, Banking and Property. For more information, please visit http://www.britam.com/

2.1 Britam Vision

To be LEADING diversified financial services company in our chosen markets across Africa.

2.2 Britam Mission

Providing you with financial security EVERY STEP OF THE WAY.

3 OVERVIW OF THE PROPOSAL

3.0 Overview

Britam has invested heavily in information technology to support its critical business operations. The IT infrastructure also incorporates state-of-the-art cyber security technologies designed to safeguard the organisation's technology investment.

Britam intends to further strengthen its cyber security posture by engaging a partner to provide a best-in-class IT Security Operations Center as well as the required processes and resources for its operation.

Britam is therefore inviting leading SOCaaS providers to submit proposals for the provision of the IT services specified in this Request for Proposal (RFP).

3.1 Objective of the SOCaaS Implementation

Britam intends to obtain the following benefits from the SOCaaS implementation:

- Overall protection of Britam's network and data from threats through monitoring, analysis and automated incident containment;
- Continuous monitoring of all aspects of the IT environment – including all endpoints, servers, desktops, business applications, databases, network devices internet traffic and more – for suspicious activity;
- Minimal time between incident occurrence and incident detection;
- Faster incident response times (with automated instantaneous containment of threats);
- Minimal impact (costs and other damages) from breaches due to fast response times;
- Continuous (24/7/365) monitoring services to contain threats regardless of the time of occurrence;
- Greater control and transparency surrounding IT security operations and procedures;
- Evidence-based reporting of risks and vulnerabilities;
- Reduced Total Cost of Ownership (TCO) for the SOC services.

3.2 Scope of Work

The expected scope of work is to monitor the Britam IT environment and publicly available data in order to detect, analyse and identify possible threats.

The successful bidder will be expected to provide all of the needed components, consultation, installation, services, subscriptions, maintenance and training to implement a fully functioning SOCaaS solution as presented in this RFP.

The explicit scope inclusions are detailed in the table below but not limited to:

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
1.	Overall Solution Expectation	Solution should be capable of delivering next generation SOC capabilities like PREDICT, DETECT & RESPOND with advanced threat hunting, monitoring, detection, auto-containment & remediation features including threat intelligence, orchestration, playbooks, automation supported by machine learning. Solution should be highly scalable and support high availability architecture.		
2.	Overall Solution Expectation	The solution should be capable of: • Collecting and analysing mirrored traffic • Collecting, storing and correlating logs • Conducting asset and vulnerability scans • Having its own threat intelligence feed and Integrating with any others using different format (STIX, JSON, etc.)		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
3.	Licensing	Provide the licensing details for the proposed solution (periodic or perpetual, licensed by seat, IP address, named-user or by events per second). Annual subscription preferred with no CAPEX.		
4.	System requirements	The solution should be capable of covering 2,000 IP addresses.		
5.	Solution Hosting	Please indicate whether the solution can be hosted both in-house and in the cloud highlighting the preferred model.		
6.	SOC Administration	The bidder should be fully responsible of administering the proposed tools (MDR, honeypots, VA etc.), including regular backup of the system, restoration, storage capacity, installation, removal, troubleshooting of any related component, health check monitoring, keeping in mind that Britam shall be allowed the same access once applied.		
7.	Log Management	Vendor to provide native & out-of-the-box supported devices as log sources along with integration methods & protocols.		
8.	Log Management	The proposed solution should have capability to integrate with unsupported/custom application/data-sources. Vendor to provide integration methods and protocols. This will		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		apply to critical Britam business applications.		
9.	Log Management	The solution should be able to integrate new data sources into existing collectors without disruption to the on-going data collection.		
10.	Log Management	Proposed solution should not lose event log data in case of network connectivity failure.		
11.	Log Management	The solution should provide proactive alerting on collection failures so that any potential loss of events and audit data can be minimized or mitigated.		
12.	Log Management	Proposed solution shall support tamper-proof preservation of raw logs and normalized data (evidence should be presentable in the court of law and nobody should have delete rights) along with capability to filter logs based on Britam requirements and ingest the logs to the security monitoring and analytics platform.		
13.	Log Management	Proposed solution shall maintain the online logs for three months, and offline retention for a period of 1 year. Solution shall purge the older log data as per the retention period. If required, vendor should upgrade the storage or any other hardware replacement.		
14.	Log Management	The solution should compress the collected log data without losing the integrity. Kindly state		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		the compression ratio and technology used.		
15.	Log Management	Proposed solution should be capable of retrieving the archived logs for analysis, correlation, reporting and forensic purposes.		
16.	Log Management	The solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service.		
17.	Log Management	All communication channels should be encrypted in line with current industry best practices.		
18.	Log Management	Encryption of stored logs - encryption level & key storage should be as per current industry best practices.		
19.	Analytics	The monitoring and analysis functionality should include adhoc, extensive and enriched information such as asset (cloud or on-premises), session, connection etc. to ensure threats can be identified beyond just devices information.		
20.	Automation & Orchestration Platform	Solution should be capable of cross-validating security events/alerts and prioritising them and triaging inbound alerts involving enriching events with additional contexts.		
21.	Automation & Orchestration Platform	a) Solution should have capability of automating indicators of compromise (IOC)		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		hunting across the Britam network and alert & take actions in case any match is found. b) For the matched IOC, asset risk score should be raised and displayed on the live dashboard.		
22.	Automation & Orchestration platform	Solution should be capable of providing data and alerts to make sure all the automated processes are running as expected. Any failures of system/process/flow should be highlighted via alerts or live dashboard.		
23.	Automation & Orchestration platform	As part of threat intelligence sharing, solution should notify Britam of all information shared with global threat intelligence platforms / open-source-community.		
24.	Automation & Orchestration platform	Solution should have extensive & growing list of integration with IT and security applications/devices/threat intelligence feeds etc.		
25.	Automation & Orchestration platform	The solution must support automated incident response & remediation through the use of playbooks covering major threats including malware/ransomware, defacement attack, DDoS, data exfiltration etc. The solution must be able to autonomously respond to and contain incidents based on rules set by Britam e.g. depending on		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		incident criticality or affected asset.		
26.	Automation & Orchestration Platform	Vendor should have capability and experience in creating and executing automation and orchestration use cases in large enterprises. The vendor should develop Incident Response Playbooks covering major threats including malware/ransomware, defacement attack, DDoS, data exfiltration etc.		
27.	Threat & Event Correlation	Solution should be able to prioritize events based on Threat score, Risk and Potential security incident or breach.		
28.	Threat & Event Correlation	Solution should be capable of providing dynamic Risk rating to users, assets and devices with multiple high risk alerts flagged from different data sources.		
29.	Threat & Event Correlation	The solution should do normalization, correlation & aggregation of any kind of log data in real time.		
30.	Threat & Event Correlation	Statistical Threat Analysis - To detect new, unknown threats and anomalies with immediate out-of-the-box value that can be improved through tuning.		
31.	Threat & Event Correlation	Susceptibility Correlation - Raises visibility of threats against susceptible hosts, Reduces noise of threats against non-susceptible hosts.		
32.	Threat & Event Correlation	Solution should provide threat scoring based on:		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		• Host, network, validity, priority for both source & destination. • Real-time threat to Britam, event frequency, attack level.		
33.	Threat & Event Correlation	The solution should provide a complete visibility into Cyber attack kill chain process - like how many attacks are in recon state, exploit state, enumerated state etc.		
34.	Threat & Event Correlation	Solution should be able to predict and take corrective action based on industry, region and country specific risk.		
35.	Threat detection	The proposed solution must be capable of detecting and reporting the suspicious traffic patterns in both, real time as well as the event/s that occurred in past based on Machine Learning / Deep Learning / Profiling mechanisms		
36.	Threat hunting	The solution should have pre-defined playbooks and run-books and should be capable of creating new ones as per Cyber Kill-Chain stages.		
37.	Threat Intelligence	The proposed solution should be able to import the vulnerability information from scanning & assessment tools on real time basis and correlate them for all possible implications.		
38.	Threat Intelligence	The solution should be able to correlate threats seen within		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		Britam with 3rd party threat intelligence sources and provide actionable threat reports. The bidder must be able to correlate logs based on threat intelligence feeds for botnet C&C servers, malware domains, proxy networks, known bad IPs and hosts, traffic to APT domains, File Information feeds including Hashes, time stamps, file size and formats, web reputation feeds including Original URL, hashes, timestamps and classification. The bidder is requested to explain how they use external data (e.g., threat intelligence feeds) to analyse potential threats to Britam's environment, and describe what access to this data Britam will have.		
39.	Threat Intelligence	Describe support for bidirectional threat intelligence using open standards, such as STIX/TAXII/OpenIoC.		
40.	Threat Hunting	Vendor should provide threat hunting services in identifying unknown patterns and creating new rules on ongoing basis.		
41.	Attack simulations	The bidder should perform cyber-attack simulations and vulnerability assessments on a regular basis (at least twice a year) to validate detection capabilities. The scope of these tests should be aligned to the SOCaaS scope.		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
42.	Event detection	Honeypots should be placed on all the environment levels (internal, DMZ, external) and integrated with the SOC.		
43.	File integrity Checks	Monitor business critical files, modification, change, accessed etc. based on business requirements and criticality. Solution should send alerts on unauthorized user access of critical files.		
44.	Forensics	Vendor should have a complete forensics investigation framework with pre-defined processes and methodologies. Vendor should provide On-Demand forensics services.		
45.	Incident Management	Proposed solution should have facility for log investigation and follow incident management lifecycle such as Incident handling, Incident containment, Incident remediation, Incident investigation, Incident recovery etc. as per ITIL standards with a search facility to search the collected raw log data for specific events or data.		
46.	Incident Management	SLA for incident resolution based on incident severity (1,2,3,4) to be provided by vendor.		
47.	Incident Management	Vendor to provide Root Cause Analysis reports (RCA) for any reported security incidents as and when requested.		
48.	Incident Management	Vendor should provide extensive incident management reporting		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		features with live dashboard on incident status.		
49.	Incident Management	Vendor should provide a ticketing tool with out of the box integration with 3rd party IT Service Management solutions.		
50.	Incident Management	The solution should have an inherent incident tracking system that can: - Track, investigate and resolve events in workflow-like environment. - Create new incidents and assign them to specific groups and users who will be notified and receive the incidents and relevant data.		
51.	Incident Management	The system must support the sending of event related notifications on SMS and email.		
52.	Incident Management	The solution should provide online and real time remediation guidance for identified security incidents.		
53.	SOC Roles & Responsibilities	Describe the terms you will be committing to through your logging and monitoring service (including SOC roles and responsibilities, time to detect incident, time to report, to respond to investigation enquiries, availability of the managed service, SOC KPIs…)		
54.	People	Vendor to provide roadmap of training/skill enhancement, cross-pollination, certifications etc.		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
55.	Operations	Vendor should present their roaster management to ensure availability of resources for 24x7x365. (leave/emergencies etc. should not affect Britam). Availability of the people should be 24*7*365 and must follow L1-L2-L3 format.		
56.	People	Vendor should provide skill matrix of people to be deployed for this project along with overall vendor skill matrix.		
57.	People	Vendor personnel shall possess the following skills: • Forensics and log analysis • Code and malware analysis (Disassembler) • Packet Analyser & Header analyser to identify threats • Information gathering • Big data & Machine learning • Incident response & tracking • Advance Analytics • Monitoring • Asset Discovery • Behavioural Monitoring • Research Tools • VA Tools • Vendor to any additional expertise other than mentioned above.		
58.	Process	Vendor should develop detailed Standard Operating Procedures (SOPs) for all major SOC processes.		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
59.	Process	Vendor to provide roadmap for solution upgrade (software/hardware).		
60.	Process	Vendor to identify measurable metrics/preparedness indicators for measuring efficacy of various operations and publish periodic dashboards.		
61.	Process	Provide daily/weekly/monthly reports covering all KPI/KRI for various stakeholders.		
62.	Process	Vendor to provide support in the timely closure of gaps identified in internal or external audits, assessment exercises etc.		
63.	Reporting	Solution should support: • Real-time reporting as well as scheduled reporting • Solution should support report designing capability without using third party products. • Vendor should design customized reports as desired from time to time.		
64.	Compliance	The solution must have out of the box compliance reporting & dashboards adhering to global standards like PCI-DSS, ISO27001, GDPR etc.		
65.	Dashboard	The reporting should give visibility into trend analysis of events, threats, alerts, vulnerabilities etc. for comparative reporting of various aspects associated with Britam		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		security posture compared with security posture best practices.		
66.	Analytics	Events can be displayed based on contextual information such as user name, preferences and event queue can be sorted easily based on majority fields such as event priority, event start time, end time, attacker IP, target IP, risk reputation etc.		
67.	Role based access rights	The system should have the ability to define various user roles, including but not limited to: • Administrator • Configuration Manager • System Auditor • Operator • System Analysts • Operators with Special additional rights • Users from Senior Management Group having access to Dashboard Reports • Custom user roles		
68.	Rules & Policies	The solution should support creation/modification of custom co-relation rules as and when required. Vendor to provide SLA for this.		
69.	System Management	Vendor should maintain system & audit logs for all the technologies going to be deployed as part of solution.		
70.	System Management	Vendor should follow Britam hardening and patching		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
		guidelines. Patching / updates of solution should be sole responsibility of solution provider / vendor.		
71.	System Management	The Solution Database should use Write Once Read Many (WORM). Once the logs are written to the disk/database no one including solution / database / system administrator should be able to modify or delete the database / system administrator should be able to modify or delete the stored raw logs.		
72.	Technology	Vendor should have malware analysis lab with sandboxing facility (please provide details).		
73.	Brand Protection	Do you perform phishing detection and how?		
74.	Brand Protection	Do you perform malware detection and how?		
75.	Brand Protection	Do you perform social media monitoring and how?		
76.	Brand Protection	Can you detect impersonation of executive staffs and how?		
77.	Brand Protection	Can you detect rogue mobile application and how?		
78.	Brand Protection	Can you detect brand abuse and how?		
79.	Brand Protection	Can you detect similar sounding domain registration and how?		
80.	Brand Protection	Do you provide spam monitoring and how?		
81.	Brand Protection	Do you provide Dark Web Monitoring and how?		

	CATEGORY	BRITAM REQUIREMENTS	COMPLIANT (YES/NO)	DETAILS AND COMMENTS
82.	Technology	Vendor should support cloud infrastructure security monitoring.		
83.	Third Party Compatibility Matrix	Vendor should provide a Compatibility Matrix for the proposed solution. This may be attached as separate document.		
84.	Auditing Capability	The solution should have the ability to track and audit the history of activities, audit trail and changes made to it.		
85.	Virtualization support	Indicate the appliance or Virtual machine to be implemented with different specs and requirements. Redundancy should be taken into consideration.		
86.	Training	Training program and documentation process should be described regarding: • Providing technical training to Britam personnel (system and security administrators) who will be using the solution. • Assurance of the quality of hardware/software documentation.		
87.	POC	Bidders should be willing to conduct a POC prior to contract award to validate the responses in their proposal. A site visit to an existing reference site may also be required.		

4 FORMAT OF RESPONSE TO TENDER

4.0 Information to be provided by bidders

All bids should contain **ALL INFORMATION REQUESTED IN SECTIONS 4.1 TO 4.5.** The information should be in the following order.

4.1 General Information about the firm

Provide the following documentation in respect of your company.

- Certification of Registration or Incorporation
- Current Trade Licence(s)
- PIN certificate
- VAT certificate as applicable

4.2 Organization of the firm

- Depth of the firm's practice in serving global clients of the scale and scope of Britam.
- Briefly highlight the profiles and technical qualifications of key staff to be involved in the project – experience in SOC deployment, MDR deployment, incident response, computer forensics.
- Statement summarizing the benefit to Britam of engaging the firm.

4.3 Reference Sites

Statement of capabilities and references in similar projects undertaken over the last three years including a brief description of the projects undertaken and reference letters. The firm needs to have conducted similar work with an insurance company in Africa of the same or bigger, size and operation with Britam.

By responding to this Tender the service provider confirms that they have no objection to Britam obtaining independent references from their current customers in furtherance of this Tender.

4.4 Particulars of the Project Deliverables

This section shall provide details including but not limited to your project methodology and major project milestones and deliverables per phase of the project as outlined in paragraph 3.2

4.5 Bid Preparation and Submission

Bid documents should be put in plain sealed envelopes labelled as below and dropped in the tender box located on 5th floor Britam Centre, Nairobi.

RFP FOR PROVISION OF IT SECURITY OPERATIONS CENTER-as-a-Service – BRITAM HOLDINGS Plc

Tenders may also be posted 7 days earlier than the deadline to:

The Procurement Manager
Britam Head Office
Mara / Ragati Road Junction, Upper Hill
P. O. BOX 30375 – 00100 NAIROBI

And marked at the top **"DO NOT OPEN BEFORE MARCH 19th 2020, 3:00 PM (GMT +3)"**

Offers must be submitted in two separate documents, a technical and commercial bid and must be submitted in separate files envelopes, clearly labelled as:

- The file with the technical proposal should be identified as follow
  NAME OF THE COMPANY, TECHNICAL PROPOSAL
- The file with commercial proposal should be identified as follows:
  NAME OF THE COMPANY, COMMERCIAL / FINANCIAL PROPOSAL

A soft copy of the bid should also be submitted on CD together with the bid documents through the tender box. No soft copy submission of the bid shall be made through any electronic means prior to the bid opening. Any such electronic submission shall lead to disqualification of the bid.

5 GENERAL CONDITIONS OF CONTRACT

5.1. Introduction

Specific terms of contract shall be discussed with the bidder whose proposal will be accepted by the Company. The resulting contract shall include but not be limited to the general terms of contract as stated below from 5.2 to 5.14.

5.2. Award of Contract

Following the opening and evaluation of proposals, the Company will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid. Britam will communicate to the selected bidder its intention to finalize the draft conditions engagement in consultation with the bidder

5.3. Application of General Conditions of Contract

These General Conditions (sections 5.2 to 5.14) shall apply to the extent that they are not superseded by provisions in other parts of the Contract that shall be signed.

5.4. Bid Validity Period

Bidders are requested to hold their proposals valid for ninety (90) days from the closing date for the submission.

5.5. Non-variation of Costs

The prices quoted for the service and subsequently agreed and into the contract shall be held fixed for the contract period.

5.6. Delays in the Bidder's Performance

5.6.1. Delivery and performance of the Transaction shall be made by the successful Bidder in accordance with the time schedule as per Agreement.

5.6.2. If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Company in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Company shall evaluate the situation and may at its discretion extend the Bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

5.6.3. Except in the case of "force majeure" as provided in Clause 5.14, a delay by the Bidder in the performance of its delivery obligations shall render the Bidder liable to the imposition of liquidated damages pursuant to Clause 5.8.

5.7. Liquidated damages for delay

The contract resulting out of this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in performance of contract.

5.8. Governing Language

The Contract shall be written in the English Language. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall also be in English language.

5.9. Applicable Law

This agreement arising out of this RFP shall be governed by and construed in accordance with the laws of Kenya and the parties submit to the exclusive jurisdiction of the Kenyan Courts.

5.10. Successful Bidder's Obligations

The successful bidder:

5.10.1. Is obliged to work closely with Britam staff, act within its own authority, and abide by directives issued by the Company that are consistent with the terms of the Contract.

5.10.2. Will abide by the job safety measures and will indemnify the Company from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Company responsible or obligated.

5.10.3. Will be responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanours.

5.10.4. Will not disclose the Company`s information it has access to, during the course of the work, to any other third parties without the prior written authorization of the Company. This clause shall survive the expiry or earlier termination of the contract

5.11. PAYMENT TERMS

Britam will not make any payments in advance. Britam will issue an LPO for all services required and the LPO will be paid 30 days from receipt of invoices in arrears.

Britam will not accept partial deliveries and neither will it make partial payments.

6 BRITAM SUPPLIER CODE OF CONDUCT

6.1 GENERAL

This Code is applicable to all Britam suppliers (hereinafter "Supplier" or "Suppliers") and their employees (be they temporary, casual or permanent) and sub-contractors throughout the world. Britam requires all Suppliers to conduct their business dealings with Britam in compliance with this Code and in compliance with all laws applicable to the Supplier's' business, wherever conducted. By entering into business transactions with Britam, the Supplier agrees to abide by the terms of this Code and acknowledge that compliance with this Code is required to maintain the Supplier's status as a Britam Supplier. Britam shall have the right to terminate any Supplier's contract for failure to comply with the provisions of this Code. Britam recognizes that local laws may in some instances be less restrictive than the provisions of this Code. In such instances Suppliers are expected to comply with the Code. If local laws are more restrictive than the Code, then Suppliers are expected to comply with applicable local laws.

6.2 PROVISIONS

In particular, Suppliers must comply with the following:

6.2.1 Relations with competitors

Suppliers will be required to comply with applicable antitrust or competition laws and will not engage in any restrictive trade practices. Suppliers will at all-time act in a manner that will uphold and encourage healthy competition. The applicable anti-trust legislation with regard to Kenya operations is the Restrictive Trade Practices, Monopolies and Price Control Act (Cap 504 Laws of Kenya).

6.2.2 Bribes, Conflicts of Interest, Gifts and other Courtesies

6.2.2.1 Bribes

Suppliers shall not make or offer bribes or payments of money or anything of value to any Britam employee or any other person including officials, employees, or representatives of any government or public or international organisation, or to any other third party for the purpose of obtaining or retaining business with Britam. For the avoidance of doubt Britam considers an act of bribery to include the

giving of money or anything of value to anyone where there is belief that it will be passed on to a government official or Britam employee for this purpose. Suppliers are required to comply with all applicable local anti-bribery laws.

6.2.2.2 Gifts and other business courtesies

Suppliers shall ensure that any expenditure incurred in relation to any particular Britam employee or government official is in the ordinary and proper course of business and cannot reasonably be construed as a bribe or so as to secure unfair preferential treatment. A general guideline for evaluating whether a business courtesy is appropriate is whether public disclosure would be embarrassing to the Supplier or Britam.

Britam employees may accept unsolicited gifts from Suppliers provided:

- they are items of nominal value – KShs 1500 or less, or
- they are advertising or promotional materials having wide distribution e.g. calendars, stationaries, diaries, etc.; and
- Acceptance of the gift does not violate any applicable law.

6.2.2.3 Conflicts of Interest

No supplier shall enter into a financial or any other relationship with a Britam employee that creates a conflict of interest for Britam. A conflict of interest arises when the material personal interests of the Britam employee are inconsistent with the responsibilities of his/her position with the company. All such conflicts must be disclosed and approval to the transaction given.

6.2.3 Compliance and implementation

6.2.3.1 Licenses and Returns

The Supplier will be required to obtain and renew, in accordance with any law or regulations all permits, licenses and authorizations

required for it to carry out its business. In addition, the Supplier will be required to prepare and file any returns that it may be required to file under its incorporation statute, the Companies Act (Cap 486 Laws of Kenya) or applicable local or Kenyan revenue legislation.

6.2.3.2 Taxation, Financial Integrity and Retention of Records

- The Supplier will comply with all revenue laws and will not evade tax.
- Suppliers will be required to maintain accurate and reliable financial and business records and shall not have any false or inaccurate accounting books or records related to Britam for any reason. Suppliers shall maintain all business records at the minimum in compliance with the provisions outlined by the Kenya Revenue Authority or local revenue authorities from time to time.
- When any government investigation or audit is pending or ongoing then Suppliers will not destroy any relevant records until the matter has been investigated and closed.

6.2.4 Violations

If a Supplier becomes aware of any known or suspected improper behaviour by another Supplier in relation to their dealings with Britam or if a bribe or other inducement is requested from a Supplier by any Britam employee or any other person with the promise of influencing Britam's position as far as that Supplier is concerned or if the Supplier feels that a conflict of interests exists with one of Britam's employees then all pertinent details should be reported in confidence to the following Contact Address

Procurement procurement@britam.com

6.2.5 Variations

Britam reserves the right to vary this Code at any time.