APPENDIX 2: SECURITY SOFTWARE REQUIREMENTS

BANK OF TANZANIA

BILL OF MATERIALS FOR TANZANIA INSTANT PAYMENT SYSTEM (TIPS) ON-PREM INFRASTRUCTURE

NETWORK SECURITY SOFTWARES

1. Supply of a Vulnerability Management Software

1.1 Description of the Software

The software to be delivered is required to enable the Bank to accurately identify potential vulnerabilities by performing Vulnerability Management software on diverse networked Information Technology devices and systems.

1.2 Scope of Work

The work to be carried out under this contract shall include:

1.2.1 Supplying the software based on specifications provided in **Annexure I** taking into account that the supplier shall recommend latest software available.

1.2.2 Providing technical support so as to ensure the software is correctly installed and works as required.

1.2.3 Providing training to a maximum of ten (10) selected Bank staff on installation, configuring and effectively using the software.

2. Supply of a Penetration Testing Software

2.1 Description of the Software

The software to be delivered is required to enable the Bank to accurately identify potential vulnerabilities by performing penetration testing software on diverse networked Information Technology devices and systems.

2.2 Scope of Work

The work to be carried out under this contract shall include:

2.2.1 Supplying the software based on specifications provided in **Annexure 2** taking into account that the supplier shall recommend latest software available.

2.2.2 Providing technical support so as to ensure the software is correctly installed and works as required.

2.2.3 Providing training to a maximum of 5 selected Bank staff on installation, configuring and effectively using the software.

3. Supply of a Security Operation Center (SOC) Software

3.1 Description of The Software

The software to be delivered is required to enable the Bank to manage Security operations on diverse networked Information Technology devices and systems.

3.2 Scope of Work

The work to be carried out under this contract shall include:

3.2.1 Supplying the Security Operations Center software based on specifications provided in **Annexure 3**. The supplier shall recommend latest software available.

3.2.2 Providing technical support so as to ensure the software is correctly installed and works as required.

3.2.3 Providing training to selected Bank staff on installation, configuring and effectively using the software.

3.3 Technical Specifications

Technical specifications for Security Operation Center (SOC) Software are in **Annexure III**.

ANNEXURE I

TECHNICAL SPECIFICATIONS FOR THE VULNERABILITY MANAGEMENT SOFTWARE

S/N	BANK'S SPECIFICATION REQUIREMENTS	
1.	**Product Name:** Tenable.Sc	
2.	**Manufacturer/Vendor :** Nessus	
3.	**VULNERABILITY ASSESSMENT**	
	The Software should have capability to:	
	1.1	Perform vulnerability assessment on the following environments:
		(i) **Operating Systems** including Microsoft Windows and various versions of Linux and Unix Servers
		(ii) **Databases** including various versions of Oracle database, Microsoft SQL, and MySQL
		(iii) Web based Applications
		(iv) **Network devices** including Firewalls, Router and switches from various Vendors such as CISCO, Huawei, and Juniper;
		(v) **Virtualized environments**: Hyper-V, VMware and Red Hat Enterprise Virtualization Hypervisors (RHEV-H).
		(vi) Wireless network devices
	1.2	Maintain logs of activities performed by various user groups
	1.3	Provide a unified portal for Vulnerability Management, Compliance Validation and Penetration Testing
	1.4	Translate vulnerability knowledge into meaningful risk metrics, i.e., it should be flexible to allow customization to suit the Bank's needs
	1.5	Fingerprint and assess vulnerabilities on mobile devices, such as, Tablet Computers and Smart Phones
	1.6	Perform vulnerability scanning on internal and perimeter network
	1.7	Provide continuous monitoring of the environment to detect for new vulnerabilities and alert designated employees
2	**NETWORK DISCOVERY, PORT SCANNING AND SERVICE IDENTIFICATION**	

	The Software should have the capability to:	
	2.1	Passively or actively discover hosts on the network without causing disruption to the hosts or the network.
	2.2	Perform port scanning on target hosts so as to accurately identify active hosts, Operating Systems, ports status and running network services.
	2.3	Support different port scanning techniques such as ability for the user to craft custom packets
3	**INTEGRATION WITH OTHER PRODUCTS**	
	The Software should be capable to:	
	3.1	Integrate with Security solutions such as Patch Management solutions, Ticketing System
	3.2	Integrate with penetration testing software
	3.3	Ability to integrate user Management with LDAP or Active Directory
4	**CONFIGURATION AND COMPLIANCE ASSESSMENT**	
	The Software should have the following features for Configuration and Compliance	
	4.1	Have a full-featured configuration compliance functionality that provides mappings from a wide list of regulations to actual IT controls
	4.2	Capability to perform configuration assessment on various environments in line with well recognized compliance framework such as **DISA STIG**, **FDCC/USGCB**, Center for Internet Security (**CIS**), **NIST SP-800**, **COBIT, ISO 27001**, **PCI** and vendor specific templates.
	4.3	Capability to establish a baseline of vulnerability conditions for network-attached devices, applications and database, identify changes in vulnerability states, and provide current vulnerability status and trends.
	4.4	Capability to provide customization of configuration templates via a graphical user interface (GUI).
INTERFACE		
The Software should have the following Interface features:		
8.1	Be Web-based with a friendly graphical user interface (GUI)	
8.2	Use secure web interface (TLS) protection	
8.3	Be capable to support various web browsers including Mozilla Firefox, Google Chrome and Internet Explorer	
REPORTS		

The Software should have the following Reporting features:	
9.1	Capability to generate predefined or customized/ad-hoc reports based on various use cases
9.2	Possess flexible and simple reporting options including scheduling report generation and delivery.
DEPLOYMENT OPTIONS	
The Software should be able to be deployed at various environments including:	
10.1	Deployed as an enterprise solutions with targeted IP addresses of 2048
10.3	Be available as a software or virtual machine that can be deployed at the client site.
10.5	Capability to run on the following environments: Linux or Microsoft Windows server environment
GENERAL REQUIREMENTS	
The Software should have the following features:	
11.1	Have a Console Manager providing role based access management, reporting/dashboards, distributed scanner deployment and workflow.
11.2	Have consolidated scanning and analysis features for deployment efficiency and simplicity
11.4	Flexibility to allow the administrator to perform scanning and analysis based on desired criteria such as IP addresses.
11.5	Capability to perform IP-based scanning
11.7	Flexibility to perform scanning with or without knowledge of credentials on the target host
11.8	Capability to support assigning of risk rating on identified vulnerabilities and providing remediation prioritization with context regarding vulnerability severity and assets criticality
11.9	Capability to provide remediation guidance

ANNEXURE 2

TECHNICAL SPECIFICATIONS FOR PENTRATION TESTING SOFTWARE

S/N	BANK'S SPECIFICATION REQUIREMENTS	
4.	**Product Name:** Core Impact	
5.	**Manufacturer/Vendor :** Core Security	
6.	**PENETRATION TESTING**	
	The Software should have capability to:	
	1.1	Perform penetration testing on the following environments:
		(vii) **Operating Systems** including Microsoft Windows and various versions of Linux and Unix Servers
		(viii) **Databases** including various versions of Oracle database, Microsoft SQL, and MySQL
		(ix) Web based Applications
		(x) **Network devices** including Firewalls, Router and switches from various Vendors such as CISCO, Huawei, and Juniper;
		(xi) **Virtualized environments**: Hyper-V, VMware and Red Hat Enterprise Virtualization Hypervisors (RHEV-H).
		(xii) Wireless network devices
	1.2	Maintain logs of activities performed by various user groups
	1.4	Validate existence of detected vulnerabilities through built-in features
	1.5	Perform different Penetration Testing techniques (through built-in features or integration with specialized penetration testing solutions), such as Web Application Testing, IDS/IPS Evasion, Firewall Evasion, Brute Forcing of authentication credentials.
2	**NETWORK DISCOVERY, PORT SCANNING AND SERVICE IDENTIFICATION**	
	The Software should have the capability to:	
	2.1	Actively discover hosts on the network without causing disruption to the hosts or the network.
	2.2	Perform port scanning on target hosts so as to accurately identify active hosts, Operating Systems, ports status and running network services.

	2.3	Support different port scanning techniques such as ability for the user to craft custom packets
3	**INTEGRATION WITH OTHER PRODUCTS**	
	The Software should be capable to:	
	3.1	Ability to imports and validate results generated by various vulnerability management software
INTERFACE		
The Software should have the following Interface features:		
8.1	Be Web-based with a friendly graphical user interface (GUI)	
8.2	Use secure web interface (TLS) protection	
8.3	Be capable to support various web browsers including Mozilla Firefox, Google Chrome and Internet Explorer	
REPORTS		
The Software should have the following Reporting features:		
9.1	Capability to generate predefined or customized/ad-hoc reports based on various use cases	
9.2	Possess flexible and simple reporting options including scheduling report generation and delivery.	
DEPLOYMENT OPTIONS		
The Software should be able to be deployed at various environments including:		
10.1	A named user licence: one user with an ability for concurrent penetration testing of 256 IP addresses	
GENERAL REQUIREMENTS		
The Software should have the following features:		
11.4	Flexibility to allow the administrator to perform scanning and validate discovered vulnerabilities.	
11.5	Capability to perform IP-based scanning	
11.7	Flexibility to perform scanning with or without knowledge of credentials on the target host	

ANNEXURE 3

TECHNICAL SPECIFICATIONS FOR SECURITY OPERATIONS CENTER SOFTWARE

S/N	BANK'S SPECIFICATION REQUIREMENTS	
7.	**Product Name:** LogRhythm Enterprise and LogRhythm Netmon	
8.	**Manufacturer / Vendor Name :** LogRhythm	
9.	SECURITY EVENT AND LOG MANAGEMENT	
	The Software should have capability to:	
	1.1	Collect and normalize logs from various sources and format including:
		(xiii) Operating Systems including Microsoft Windows and various versions of Linux and Unix Servers
		(xiv) Databases including various versions of Oracle database, Microsoft SQL, and MySQL
		(xv) Network services including Active Directory, DHCP, DNS, VPN, SSL-VPN, proxy servers.
		(xvi) Applications
		(xvii) Network devices including firewalls, router and switches from various Vendors such as CISCO, Huawei, and Juniper
		(xviii) Virtualized environments: Hyper-V, VMware and Red Hat Enterprise Virtualization Hypervisors (RHEV-H).
		(xix) Wireless network devices
	1.2	Ability to perform text searching or advanced searching using custom queries through log data
	1.3	Providing alerts based on pre-defined criteria
	1.4	Generating on-demand logs from a specified assets
	1.5	Track asset resource utilization such as CPU, memory and storage
	1.6	Ability to provide alerts based on pattern matching
2	THREAT INTELLIGENCE	
	The Software should have the capability to:	
	2.1	Have built-in features which provide the following intelligence that is relevant to the financial sector:
		(i) Real-time phishing attacks before sites are visited
		(ii) Web content classification to keep users safe from online threats

		(iii) Publishing dynamic intelligence of high-risk IP addresses for both inbound and outbound communication
		(iv) Dynamic file reputation intelligence of known malware
		(v) Categorizing and scoring mobile apps to ensure they are safe
	2.2	Trap attackers through the use of deception techniques such as honeypot
	2.3	Receive and utilize threat intelligence from various external sources
3	**NETWORK FORENSIC**	
	The Software should have the capability to:	
	3.1	Capture and store network packets traversing across the network. Captured data shall include source and destination, protocol used and volume of data communicated.
	3.2	Collect NetFlow data on each network connection
	3.3	Collect security events generated by Intrusion Detection Systems (IDS), Firewalls and Netflow devices
4	**INCIDENT DETECTION AND RESPONSE**	
	The Software should have the capability to:	
	4.1	Detect cyber security breaches prioritized in accordance to business impact
	4.2	Track security incidents
5	**INTEGRATION WITH OTHER PRODUCTS**	
	The software should be capable to:	
	5.1	Integrate with Security Vulnerability Management and penetration testing software
	5.2	Integrate with endpoint security products
6	**INTERFACE**	
	The Software should have the following Interface features:	
	6.1	Be Web-based with a friendly graphical user interface (GUI)
	6.2	Use secure web interface (TLS) protection
	6.3	Be capable to support various web browsers including Mozilla Firefox, Google Chrome and Internet Explorer
7	**REPORTS**	
	The Software should have the following Reporting features:	

	7.1	Capability to generate predefined or customized/ad-hoc reports on security-related incidents and events for various use cases
	7.2	Possess flexible and simple reporting options including scheduling report generation and delivery.
8	DEPLOYMENT OPTIONS	
	The Software should be able to be deployed at various environment including:	
	8.1	Deployed as an enterprise solutions with unlimited IP scanning capabilities
	8.3	Be available as a software or virtual machine that can be deployed at the client site.
	8.4	Capability to run on the following environments: Linux or Microsoft Windows server environment
9	GENERAL REQUIREMENTS	
	The Software should have the following features:	
	9.1	Have a console providing role based access management and reporting.
	9.2	Have a dashboard that easily presents an enterprise security posture. Thus, the dashboard to include potential threats facing the organization, vulnerabilities.
	9.3	Real-time visibility of individual, groups of assets or entire IT assets of Bank

ANNEXURE 4

TECHNICAL SPECIFICATIONS FOR WEB APPLICATION FIREWALL

S/N	BANK'S SPECIFICATION REQUIREMENTS	
1.	**Product Name:** F5 Advanced WAF	
2.	**Manufacturer/Vendor :** F5 Networks	
3.	**Number of WAF Instance Deployment:** Three	
3	PRODUCT FEATURES	
	The WAF should have the following features:	
	3.1.	Ability to protect web applications against automated attacks
	3.2.	Protect Web applications against attacks that target critical vulnerabilities including OWASP top ten vulnerabilities
	3.3.	Ability to defend the application against Denial of Service (DOS/DDOS) attacks
	3.4.	Protect Web applications against attacks that steal credentials, use brute-force attacks or any attacks that are based on stolen credentials
	3.5.	Ability to protect applications against threats that target APIs
	3.6.	Provide protection against attacks that involving copying of large amount of data from the application
	3.7.	Protection of application against pharming attacks
	3.8.	Ability to inspect all inbound traffic to detect malicious events
	3.9.	Ability to inspect all outgoing traffic to detect for malicious transportation of sensitive data. It should be able to block the communication upon detection of transportation of sensitive data
	3.10.	Deploy various technique for detection and prevention of attacks. These may include signature based and machine learning as well as behavioral analytics
	3.11.	Ability to provide alerts to relevant users upon detection of critical risk events based on predefined criteria
4	REPORTS	
	1.1.	Provide a graphical user interface with dashboards, summaries and details reports to meet various use cases. This may include summary

		and details insight on compliance, malicious activities, and general usage of the applications
5	DEPLOYMENT OPTION	
	5.1.	The WAF should be flexible to be implemented on hypervisor or private cloud environment based on openstack