Terms of Reference
for
Project Implementation Consultancy Firm
for Implementing National Security Operations Center (N-SOC)

1. Introduction:

Cyber security threats are increasing and irrespective of the size of an organization, many have fallen victim. With major security breaches, fraud incidents and advanced persistent threats making headlines, every type of organization has to take steps to address the growing problem of malware, spoofing, social engineering, advanced threats, fraud, and insider attacks. To defend against such threats, every organization must have good security incident detection and response capabilities.

In today's digital environment, Information Technology (IT) security is becoming a complex matter. Implementation of proper defensive mechanisms in order to mitigate these risks is a constant challenge for security experts.

Just doing traditional data source monitoring of logs, events, flaws, network traffic and alerts might not be sufficient. Multiple approaches are needed to keep up with the ever-changing threat landscape. These could include signatures/blacklists, behavioral models, algorithmic, threat intelligence and forensics with big data security analytics.

The Security Operations Center (SOC) orchestrates multiples roles, processes and technologies to enable efficient incident detection and response. It collects and analyzes cyber threat intelligence to gain insight into adversaries and their motivations, intentions, and methods.

Security and privacy incidents can greatly impact any organization's operational effectiveness and can hinder the organization's ability to complete its mission. The Primary goal of a Security Operation Center (SOC), or a Security Monitoring Infrastructure, is to provide the capability to detect and analyze potential information security and privacy related incidents.

2. Background:

Information infrastructure development has been identified as one of the key areas towards achieving the national policy objective of digitizing the economy. Usage of computer networks and applications will increase rapidly, and it is essential to ensure the confidentiality, integrity , availability and convenience of these systems and applications for building the trust of the users.

As the Government of Sri Lanka rolls out its electronic on-line citizen services such as the e-Revenue license, e-Population register, Electronic Travel Authority (ETA) (with several other initiatives planned to be implemented in 2016 and beyond), it will enable citizens to avail themselves of government services without having to make a long commute to the city. These e-Government services need to be delivered in a secure manner without any interruptions due to malicious activities against the service infrastructure. Ensuring the trust among the general public with regard to the electronic services delivered by the government is also important.

It also emphasizes the need for security during electronic service delivery, as indicated by Government web portal and web sites, which states, “Government organizations should ensure sufficient security for their web sites to ensure the integrity of the information made available and to prevent unauthorized modifications, amendments, deletions, and other malicious attacks”.

Constant monitoring and analysis of cyber risks could transform security into a business enabler, rather than a problem. Monitoring and Analytical services of a Security Operations Center help to establish proactive cyber security capabilities around the clock with actionable alerts, identification of suspicious activities and forensic investigation.

Currently, there is no national level security operations center in Sri Lanka to monitor and identify potential information security threats.

ICTA and Sri Lanka CERT plan to implement a National Security Operations Center (N-SOC) as a key national initiative aligned with digital infrastructure development projects. This will be useful in identifying and overcoming barriers in cyber security threat detection in a proactive manner while ensuring the security and availability of digital infrastructure.

3. Objective of the Assignment:

Setting up of a National Security Operations Center (N-SOC) has been proposed to monitor and identify cyber threats against both government and private sector information systems while taking preventive actions to help deliver online services in a secure manner and protecting the good image of our country.

Setting up of the National Security Operations Center is a complex task and it requires highly skilled professional approach. Therefore, this assignment intends to engage a consultancy firm for articulating the requirements, compiling the best practices to be adopted and supervising the implementation while ensuring that the standards have been followed for setting up of N-SOC.

4. Scope of Work:

The selected consulting firm should perform a study about the requirement and suggest the most appropriate solution to the ICTA and Sri Lanka CERT to build up a scalable National Security Operation Center (N-SOC). Primarily, this should involve Security Analytics, Vulnerability Management, Incident management, and digital forensics capabilities. Outlined below is the Scope of Work, (but is not limited to) for the consultancy firm;

- Study the current status and requirement of N-SOC.
- Propose SOC processes and procedures.
- Development of an action plan / road-map to develop skills and capacities of people, strategies, technologies and processes, Development of physical and logical design and Defining of specifications necessary for implementing SOC.
- Create deployment models, architecture and designs.
- Assisting for drafting the bidding documents and evaluation criteria.
- Defining the structure, roles and responsibilities of SOC team.
- Supporting development of policies and documentation.
- Facilitating recruitments and trainings.
- Supervising the SOC implementation.
- Verification of the deployed solution and propose corrective measures and recommendations for the areas with negative verification results.
- Supporting operations and sustainability arrangements.
- Facilitating the pilot operations.
- Facilitating OAT/UAT.

Below section provides high-level overview of some of the key activities

4.1 Proposed methodology for NSOC setup

Based on the initial study of the National Security Operations Center infrastructure, consulting firm will have to suggest the detailed N-SOC implementation methodology acceptable to the ICTA and Sri Lanka CERT aligned with the time lines and other criteria.

4.2 Systems Standards and Technology Road-Map

The system standards and a technology road-map have to be established which will be essential for smooth implementation and continuity of the SOC solution.

4.3 Implementation and Integration

- The consulting firm is responsible for ensuring that the SOC solutions and operations comply with all relevant, leading industry standards such as (but not limited to) ISO 27001, ISO 22301, etc. and any applicable laws and regulations in the country.
- Optimizing security technologies, personnel and processes to work together and for scaling security capabilities to increasing risks posed by advanced cyber threats.
- The consulting firm is responsible for ensuring that all devices and software are properly configured and hardened.
- Ensure that necessary information security measures are implemented in the proposed SOC.
- Develop comprehensive documentation for the operation, integration and customization of the solutions.

4.4 Security Analytics

The security analytic solutions such as Security Information and Event Management (SIEM) is expected to collect logs from network devices, servers, application security logs, anti-virus, proxy server, access control system, etc. and gives security personnel some level of visibility of what is going on across the enterprise by connecting the dots between anomalies within the different layers of defense via logs.

However, Log-centric SIEMs are unable to detect and investigate attack techniques such as unusual client activity, protocol anomalies, unauthorized connections, and suspected malware activity and hence it cannot provide deep visibility and details to understand what is truly happening in an environment.

Big Data security analytics tools (2nd generation SIEM) have the potential to provide significant advantage in actionable security intelligence by reducing the time for correlating, consolidating, and contextualizing diverse security event information, and also for correlating long-term historical data for forensic purposes. These technologies are evolving continuously.

The consulting firm is expected to provide the best suitable solution depending on the requirements of proposed N-SOC.

4.5 Vulnerability Management (VM) Tool

The solution should be capable of monitoring the infrastructure asset vulnerabilities along with the location of such vulnerabilities and suggest the mitigation steps. VM tool has to be integrated with the SOC software solution, Incident management and security dashboard.

4.6 Physical Space

The proposed N-SOC should maintain its own physical space in a secure facility. Consultancy firm should provide necessary specifications, guidelines in selecting the location. The development and improvements of the location will have to be supervised by the firm in collaboration with ICTA.

4.7 Development of Specifications for the SOC solution

Based on the above attributes, the consultancy firm should develop specifications for the entire SOC solution aligned with the priorities and implementation time-lines.

4.8 Configuration, Deployment and Integration

The consultancy firm should be responsible for liaising with the hardware and software suppliers/ SOC solution provider and should supervise and verify the configurations and deployments. Final integrations should be verified.

4.9 Training

The selected consulting firm has to arrange a detailed and hands on induction training to the persons nominated by the ICTA and Sri Lanka CERT.

The training should include the architecture, hardware, software, integration, customization, policy installation, trouble-shooting, reporting and other aspects of the system. Moreover, the firm shall create a comprehensive training plan for 3 years, and should provide initial training for the hired SOC staff.

4.10 Staff Recruitments

The consultancy firm should assist ICTA and Sri Lanka CERT in finalizing the profiles and staff recruitments

4.11 Pilot Operations

After finalizing all critical and mandatory requirements, pilot operations should continue and the consultancy firm should facilitate this. This should include all technical and operational aspects of N-SOC.

4.12 Acceptance of the SOC solution

The consultancy firm should facilitate the final acceptance of the SOC solution. Corrective measures and recommendations should be provided by the consultancy firm until the complete SOC solution meets the acceptable criteria.

4.13 Transition, Live Operation and Documentations

The transition process should be planned and all necessary documentations should be provided.

4. Deliverables and Time-line:

The consultancy firm is required to submit/complete the following list of deliverables/activities.

No	Deliverable/Activity	Time-Line
1	Kick-off	Complete by [ED+1 week]
2	Requirement document for N-SOC	Complete by [ED+2 weeks]
3	N-SOC solution Design and Architecture	Complete by [ED+ 4 weeks]
4	List of requirements for selecting a physical location and infrastructure design	Complete by [ED+ 4 weeks]
5	Specifications for SOC solution with Standards and Technology Road-Map	Complete by [ED+ 4 weeks]
6	Staff Hierarchy, Profiles, selection criteria and other procedures	Complete by [ED+ 4 weeks]
7	N-SOC Process, operation and all related manuals	Complete by [ED+12 weeks]
8	Analyst and Other Engineering Training	Complete by [ED+22 weeks]
9	Supervise and verify the configurations and final integrations of SOC solution	Complete by [ED+28 weeks]
10	Facilitate User Acceptance Testing (UAT)	Complete by [ED+30 weeks]
11	Facilitate Pilot Operations	Complete by [ED+34 weeks]
12	Facilitate Operational Acceptance Testing (OAT)	Complete by [ED+40 weeks]

ED – Contract Effective Date

5. Qualifications of the KEY CONSULTANTS;

Preferred Qualifications;

- Project consulting team

Key Professional Staff	Academic and Professional Qualifications	Experience in the PROPOSED ROLE	Experience in working in National /Enterprise level projects
Project Manager	B.Sc or equivalent and CISSP or CISM and ITILv3 or PMP Certification	5 years	3 projects
Certified Security Consultant	B.Sc or equivalent and SANS / (ISC)2 / EC-Council or Other Certified Security Certification	3 years	3 projects
Systems Architect	B.Sc or equivalent and Certification MCSE / RHCE	3 years	2 projects
Senior Network Engineer	B.Sc or equivalent and Vender Certificates related to Networking	3 years	2 projects
Senior Information Security Engineer	B.Sc or equivalent and CISSP/CEH/CCNA/CISM/ MCSE/RHCE Certification	2 years	2 projects
Information Security Auditor	B. Sc or equivalent and CISA	2 years	1 projects
Senior Business Analyst	B. Sc or equivalent	3 years	2 projects
Quality Assurance Manager	B. Sc or equivalent	3 years	1 project

6. Services and Facilities Provided by ICTA and Sri Lanka CERT|CC.

- Desk space with Internet connectivity will be provided at ICTA office for 3 individuals. Meetings with government and other organizations will be facilitated.

7. Review Committees and Review Procedures

The consultancy firm is required to work closely with the team at ICTA and Sri Lanka CERT|CC and/or any other review committee(s) as appointed/decided by ICTA/Sri Lanka CERT|CC.

All versions of deliverables will be reviewed and the acceptance will be given once the deliverables meet the acceptance criteria. All activities will also be supervised and signed-off by ICTA and Sri Lanka CERT|CC and/or any other committee(s) as appointed/decided by ICTA/Sri Lanka CERT|CC.