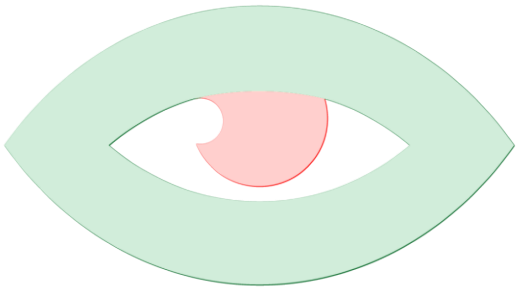
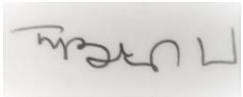
BGD E-GOV CIRT SERVICE CATALOGUE



BGD e-GOV CIRT

Bangladesh Computer Council

Signed : 

1 Table of Contents

2 Introduction

BGD e-GOV CIRT mission is to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh, which will make these programs more efficient and reliable.

Main objectives of the BGD e-GOV CIRT are:

- Manage Cyber Security in Bangladesh Government & Private sector as National CIRT (current responsibility)
- Manage cyber security in Bangladesh government's e-Government network and related infrastructure;
- Serve as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders;
- Make efforts to establish national cyber security incident management capabilities in Bangladesh.

3 Services of BGD e-GOV CIRT

In order to accomplish its mission, BGD e-GOV CIRT provides following services to its constituents:

3.1 Proactive Services

Security assessments: BGD e-GOV CIRT is constantly doing vulnerability assessments and penetration testing on assets located at the National Data Center as well as these activities can be provided to the constituency on a special official request

Configuration and maintenance of security tools, applications, infrastructures, and services: BGD e-GOV CIRT maintains described set of security tools primarily used for logs collection and archive for assets located in the National Data Center which allow to trace incidents when they occur.

Intrusion detection: BGD e-GOV CIRT collects cyber security threat information (compromises, accessible vulnerabilities) from various external feeds, filters and distributes them among the constituency.

Security consulting: BGD e-GOV CIRT provides advice and guidance on the best security practices to implement for constituents' business operations.

Awareness building: BGD e-GOV CIRT seeks opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

Cyber Sensor: Detecting intrusion, suspicious activity & development of methodology of assessing maturity level of Critical Information Infrastructure in Bangladesh government IP network, thus sensor network is being implemented.

3.2 Reactive Services

Cyber security incident handling: BGD e-GOV CIRT receives information regarding cyber security incidents, triage incidents and coordinate response. The incident handling unit provides following services:

- Vulnerability Assessment
- Penetration Test
- Incident Analysis
- Security Threat Notification
- Incident Coordination

Digital Forensic Lab: BGD e-GOV CIRT is now capable of recovery and investigation of material found in digital device including mobile, PC, Drone or any IOT's or computational devices. Service Workflow follows:

- Evidence Detection
- Evidence Acquisition
- Evidence Analysis/Examination
- Documenting and Reporting

4 About the proposal

BGD e-GOV CIRT is extending its service to all the Government, Non-Government & Semi-Government organizations. The proposal with service details of all services of BGD e-GOV CIRT are listed below. Notable points regarding the proposals are:

- All the fees are in BDT
- All the fees are excluding of any local VAT/TAX/AIT
- All the fees of Cyber Sensor Unit are excluding of any customs duty/levy/Clearing & forwarding agency charge/transportation of goods charge

5 Cyber Sensor Unit

5.1 Introduction

Detecting intrusion, suspicious activity & development of methodology of assessing maturity level of Critical Information Infrastructure in Bangladesh government IP network, thus sensor network is being implemented.

5.2 Benefit

The major benefit for deploying cyber sensor is "Identify Cyber security threats" inside the organization (where the cyber sensor is placed), for example monitor the IP network activity, finding unwanted traffic in network, suspicious/malware related executables downloads into the network. Cyber sensor also provides fast indexing and graphical review platform to index all events for deeper analysis.

5.3 Cyber sensor provides below major services

a. Manual attack traffic patterns analysis and incident detection (threat hunting)
b. Suspicious Traffic analysis
c. Anomaly detection
d. indexing and graphical review platform to index all events for deeper analysis

5.4 Professional Certifications of Team

OSCE, OSCP, SLAE-32, C|CISO, CEH, CCNP (R&S, SP), CCIP, CCNA(R&S), HCSI(R&S), RHCE, EISM, HCNP, CCNA, MCTS

5.5 Service Offer

Sl.	Service detail	Package name	Fee
1.	Installation and Commissioning of One (one unit) Cyber Sensors with 1G (ONE GE) Interface capacity	One-unit Cyber sensor Installation and Commissioning -1G Interface Capacity (One Time)	12,000,000.00 (One Time)
2.	Installation and Commissioning of One (one unit) Cyber Sensors with 10G (TEN GE) Interface capacity	One-unit Cyber sensor Installation and Commissioning – 10G interface capacity (One Time)	15,000,000.00 (One Time)
3.	Operations, Maintenance and monthly sensor report for One-unit Cyber sensor Per month	Operations, Maintenance, monthly sensor report one unit per month (Per month)	300,000.00 (Per month)

6 Risk Assessment Unit

The Cyber Risk Assessment is an essential preventive measure that effectively mitigates the possibility of the organisation's future cyber risks and challenges. The evaluation process relies on an awareness of the critical resources that might be impacted by the danger or weakness. The purpose of a risk assessment is to consider and classify threats by review of information and data obtained from existing systems and the operational environment.

6.1 Tasks to be performed

Under the package following task will be performed:

Criticality assessment – Critical assets identification of the organization
Threat adjustment for assets: Determine the relevant threats, prioritize threats from the threat catalogue and Map threats to Assets
Control strength adjustment: This step assesses the effectiveness and adequacy of controls in relation to the identified threats
Assessment of security controls: Evaluate current state of implementation of security controls of the Organization based on international threat reports and standards
Risk identification and recommendation: Prioritize risk and provide risk mitigation recommendation following international best practices.

6.2 Professional Certifications of Team

C|CISO, CEH, ISO27001 Sr. Lead Auditor, CLPTP, ITILF, COBIT5, Access Data Certified Examiner (ACE), OSFTC, CDCP, PCSS (Germany), International Law in Cyberspace (Germany)

6.3 Service Offer

Sl.	Service detail	Package name	Fee
1.	Risk assessment per Organization within Dhaka Duration: 3 weeks minimum (5 days onsite & 2 weeks offsite)	RA_DHK_01	7,00,000.00
2.	Risk assessment per Organization outside Dhaka Duration: 3 weeks minimum (5 days onsite & 2 weeks offsite)	RA_OUTDHK_01	9,00,000.00
3.	Training on Basic Risk Assessment Duration: 03 Working days Maximum Participants: 10 Person Venue: BGD e-GOV CIRT Premise	RA_Training_Basic	60,000.00
4.	Training on Advanced Risk Assessment Duration: 05 Working days Maximum Participants: 10 Person Venue: BGD e-GOV CIRT Premise	RA_Training_Advance	1,00,000.00

7 IT AUDIT Unit

7.1 Auditor(s) To Do List for the customers

Sl.	To-Do List	Pricing Modality
1.	Performing Audit	As per Section 2 below
2.	Prepare Audit Scope	As per Section 2 below
3.	Preparing Audit Framework for specific customer	As per Section 2 below
4.	Consulting with the documentation gap filling	As per Section 2 below
5.	Preparing Audit Engagement Letter and/or Audit charter	As per Section 2 below
6.	Preparing Audit Terms of Reference (TOR) for the resources	As per Section 2 below
7.	Future Predictive or future roadmap to the customer for complying with the next Audit period	As per Section 2 below
8.	Conducting Training	As per Government rule
9.	Not limited to above	

7.2 Professional Certifications of Team

CISM, CISA , ISO/IEC 27001 Lead Auditor, ITIL , Oracle Solaris 10 Certified Professional , EC Council Network Security Administrator , Oracle Linux 5 Administrator, Sun Storage 6000 Arrays Support Consultant CEH, ISO 27032 LCM, CLSSBB, CTIA, PRINCE2 Practitioner, CLPTP

7.3 Billing Part for every Audit

Sl.	Service detail	Package name	Fee
1.	Audit assessment & Reporting per Organization within Dhaka	ITAUDIT_DHK_01	8,00,000.00
	Duration: 4 weeks minimum (5 days onsite & 3 weeks offsite)		
2.	Audit assessment per Organization outside Dhaka	ITAUDIT_OUTDHK_01	10,00,000.00
	Duration: 4 weeks minimum (5 days onsite & 3 weeks offsite)		
3.	Training on Basic Information Security and Process Audit (Without Global Certification)	ITAUDIT_Training_Basic_DHK	250,000.00
	Duration: 05 Working days		
	Maximum Participants: 10 Person		
	Venue: BGD e-GOV CIRT Premise		
4.	Training on Basic Information Security and Process Audit (Without Global Certification)	ITAUDIT_Training_Basic_OutDHK	350,000.00
	Duration: 05 Working days		
	Maximum Participants: 10 Person		
	Venue: Client Premise		

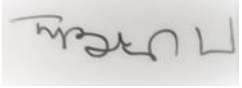
- During audit final reporting time (under the jurisdiction of auditor(s)) will be under the billing modality
- Per Day Audit work will be considered as per customer's office hour.

7.4 Activity List for every Audit

Sl.	Assignment components	Calendar days
1.	Entrance meeting	0.50
2.	Audit planning	0.50
3.	Audit execution	As per the agreement with the customer and agreed scope
4.	Closing meeting	1.00
5.	Draft report submission	As per the agreement with the customer and agreed scope
6.	De-briefing	As per the agreement with the customer and agreed scope
7.	Final draft report submission	As per the agreement with the customer and agreed scope
8.	Remarks on final draft report by customer	As per the agreement with the customer and agreed scope
9.	Final report submission	As per the agreement with the customer and agreed scope
	Total working days	**Summation S No 01 to 09**

7.5 Requirement from Auditor(s) of project

1. Purchase sampling tools for sampling the population
2. Land phone
3. Printer, Scanner, Photocopy machineries, required papers and stationeries



8 Incident Handling Unit

8.1 Introduction

BGD e-GOV CIRT receives information regarding cyber security incidents, triage incidents and coordinate response. The incident handling unit provides following services:

- **Vulnerability Assessment**
  Constantly performing vulnerability assessment to finding and measuring the severity of vulnerabilities on assets located at the National Data Center as well as these activities can be provided to the constituency on a special official request.
- **Penetration Test**
  Performs penetration test to breach security defenses on assets as well as provides the remediation for vulnerabilities by signing rules of engagement with constituency.
- **Incident Analysis**
  Analyze incident evidence to find out the root cause of how the attack has been made by the attacker and provides the best practice guidance in order to prevent further attacks.
- **Security Threat Notification**
  Receives cyber security threat information like zero-day vulnerability, malware information, ransomware infection details etc. from trusted sources, filters and distributes them among the constituency.
- **Incident Coordination**
  Receives incident notification related to BGD e-GOV CIRT's constituent networks from trusted CERT communities and forward those incidents to the concern constituents for mitigation.

8.2 Benefits

- Discover the security flaws of the assets.
- Measure security defenses against cyber attacks.
- Mitigate the potential damage after a security incident.
- Strengthen your security defenses against future incidents with lessons learned.
- Be prepared for advanced cyber-attacks by receiving threat notifications.

8.3 Professional Certifications of Team

OSCP, RHCA, CEH, EISM, Acunetix, ACE, RHCE OpenStack, RHCSA OpenStack, RHCVA, RedHat Cloud Storage, RedHat Hardening, RHCE, RHCSA, CCNA

8.4 Service Offer

Sl.	Service detail	Package name	Fee
1.	Server VAPT (Per Server) **Description**: Vulnerability assessment and penetration test on server operating system. This is a black box test which doesn't require user credential and this test will identify possible installed services, running services, open ports, service version detection, network communications, patch information etc.	SERVER_VAPT	46,000.00
2.	Website VAPT (Per Domain) **Description**: Vulnerability assessment and penetration test on website to detect possible vulnerabilities. This VAPT doesn't require user credential. This test will identify web technologies and versions, SQL injection, Cross-site scripting, Unrestricted file upload, Web backdoor, Directory traversal etc. **Note:** Each unique sub-domain will consider as domain.	WEBSITE_VAPT	1,11,000.00
3.	Web Application VAPT (Per Domain) **Description**: Vulnerability assessment and penetration test on web application to detect possible vulnerabilities. This test may require web application user credential to conduct vulnerability assessment to detect SQL injection, Cross-site scripting, Unrestricted file upload, Local or remote file inclusion, Authentication bypass, Misconfiguration etc. **Note:** Each unique sub-domain will consider as domain.	WEB_APPLICATION_VAPT	1,63,000.00

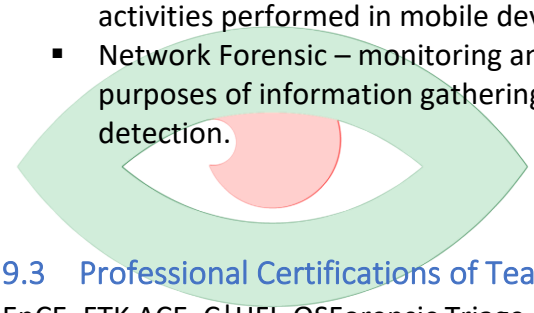
9 Digital Forensic Unit

9.1 Benefits

- Helps the incident handling unit as reactive service after an incident occurs by providing forensic support on evidence.
- Build capacity of students and government officials on Cyber Security
- Criminal prosecutors – Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- Civil litigation- Personal and business data discovered on a computer can be used in fraud, harassment or discrimination cases
- Financial Organizations – Evidence discovered on computer can be used to mollify costs
- Law enforcement officials – Rely on computer forensics to backup search warrants and post-seizure handling

9.2 CIRT Lab Capabilities

- Computer Forensic – Can be used to recover important data, deleted logs, any criminal activities which is deleted intentionally
- Mobile Forensic – Mobile device forensic investigation to detect any criminal activities performed in mobile device
- Network Forensic – monitoring and analysis of computer network traffic for the purposes of information gathering of network anomaly, legal evidence, or intrusion detection.

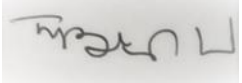


9.3 Professional Certifications of Team

EnCE, FTK ACE, C|HFI, OSForensic Triage, C|CISO, E|ISM, RHCE, Certified Cyber Defender Associate (Malaysia), International Law in Cyberspace (Germany).

9.4 Service Offer

Sl.	Service detail	Package name	Fee
1.	Component: **Computer Forensic** Duration: Min 5 working days / case Description: Evidence Detection Evidence Acquisition Evidence Analysis/Examination Documenting and Reporting	COMPUTER_FORENSIC	6,50,000.00 /CASE
2.	Component: **Mobile Forensic** Duration: Min 7 working days / case Description: Evidence Detection Evidence Acquisition Evidence Analysis/Examination Documenting and Reporting	MOBILE_FORENSIC	4,00,000.00 /CASE
3.	Component: **Forensic Support Service** Duration: Min 2 MAN days Description: On premise Forensic Technical Support Technical support on Forensic Data Acquisition Technical support on Forensic Data Analysis & Reporting Note: Forensic Tools are not included in the service, Client must provide the tools. For services including tools please refer to 1 & 2.	FORENSIC_SUPPORT	30,000.00 /Per 2 MAN Days
4.	Component: **Digital Forensics Training** Duration: 3 days (3 hours per class) / batch (total 9 hours minimum) Mode: On premise, hands on training. Tools: Open source. Participant: 20 persons / batch Note: participant's stationary & snacks arranged by inviting authority.	FORENSIC_TRAINING	22,500.00 /per batch



10 Cyber Gym Unit

Cyber Gym is essential for organizing training and build awareness on Cyber Security. It helps organizations to mitigate future cyber risks and challenges. Here we are arranging two types of training programs.

1. Three days training on basic cyber security
2. Five days training on advance cyber security.

10.1 Cyber Gym Capabilities

- Simulate Cyber Attack— Simulating latest and popular cyber attack for training purposes.
- Simulate Cyber Defense – Investigating cyber attack or criminal activities

10.2 Professional Certifications of Team

CEH, ITIL, RHCSA, RHCE, ISO 27001, PRINCE II, ISTQB Certified Tester

10.3 Service Offer

Sl.	Service detail	Package name	Fee
1.	Component: Basic Cyber Security Training Duration: 3 working days Description: ▪ Maximum 10 number of participants ▪ Basic attack and basic defense scenario simulation ▪ Basic cyber security awareness	Basic_Cyber_Security_ Training	60,000.00
2.	Component: Advance Cyber Security Training Duration: 5 working days Description: ▪ Maximum 10 number of participants ▪ Advance attack and advance defense scenario simulation ▪ Hands on training on Kali	Advance_Cyber_Security _Training	95,000.00

11 Threat Intelligence Service

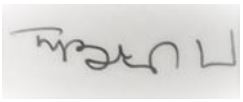
BGD eGov CIRT in association with global partners receive various threat intelligence through relevant sources. These threat intelligences may be subscribed by CIIs, Banking and Financial Institutions for assuring cyber security in their domain.

11.1 Service Offer

Sl.	Service detail	Package name	Fee
1	▪ Threat Intelligence will be provided to the entities such as Critical Information Infrastructures, Banking and Financial Institutions, Law Enforcement Agencies etc. ▪ Domain /entity based threat received from multiple sources will be provided on monthly basis. ▪ Critical threat intelligence will be shared as and when received. ▪ This service is purely on subscription basis.	Cyber Threat Intelligence	BDT 1,00,000 per month. Minimum Subscription 1year.

12 Point of contact

For any queries regarding the proposal, please reach out to:



Mr. Tarique M Barkatullah

Director (CA Operation & Security) & Director (Data Center)

Project Director, Strengthening of BGD e-GOV CIRT Project

E-mail: tarique.barkatullah@bcc.gov.bd