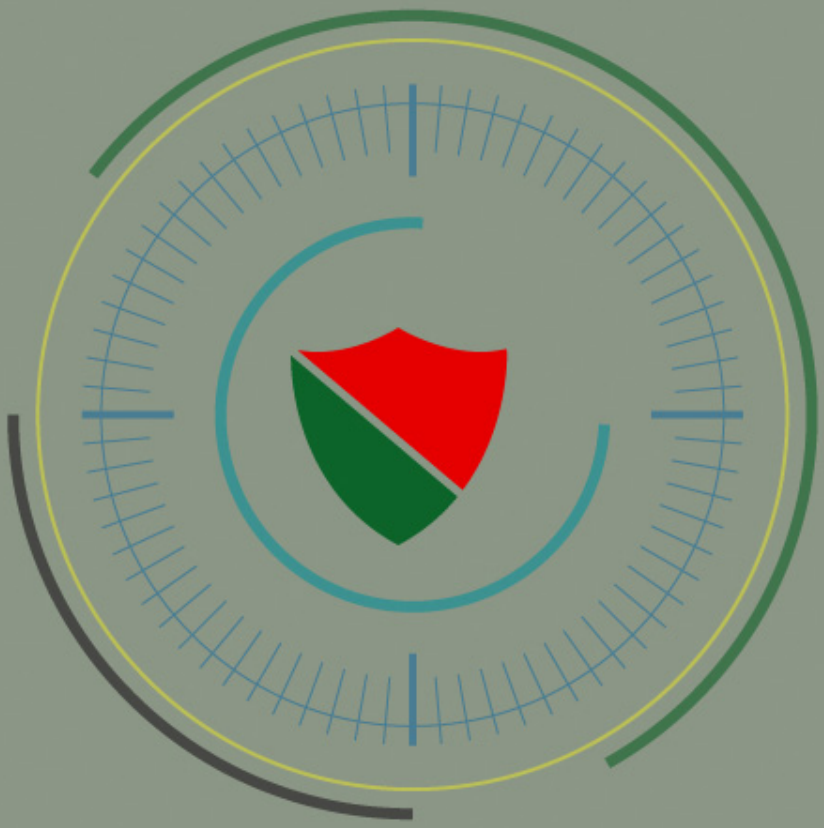
DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

BGD e-GOV CIRT

CYBER SECURITY INSIGHTS & ALERTS

BGD E-GOV CIRT

[Computer Incident Response Team]



ICT DIVISION
FUTURE IS HERE

Monthly Magazine
August 2020

Bangladesh Computer Council

Table of Contents

WHO WE ARE 1

BGD e-GOV CIRT Services 2

BGD e-GOV CIRT Membership 2

BGD e-GOV CIRT At-A-Glance 3

BGD e-GOV CIRT Insights 4

BGD e-GOV CIRT Other Services 6

- Bangladesh National Digital Architecture (BNDA) 6
  - BNDA Components 6
  - BNDA Digital Services 7
  - Global Awards & Recognitions 7
- e-Recruitment System 8
  - Features 8
  - Benefits 8
- Food Grain Procurement System (FPS) 9
  - Features 9
  - Benefits 9
- অনিরাপদ ই-মেইল থেকে কিভাবে সুরক্ষিত থাকবেন 10
  - সূচনা 10
  - ই-মেইল ঠিকানা ও ই-মেইলের বিষয়বস্তু লক্ষ্য করুন 10
  - সন্দেহজনক ই-মেইল এর সংযুক্তি ও লিঙ্ক এড়িয়ে চলুন 12
  - সর্বদা সক্রিয় ও হালনাগাদ অ্যান্টি-ভাইরাস ব্যবহার করা 14
- Data Center Management Best Practices 16
- Standard Operating Procedure (SOP) of National Data Center [Approved] 18
  - Purpose 18
  - Scope 18
  - Introduction 18
  - NDC Access Procedure 18
  - Approval Procedure of Service Requests 21
  - Equipment in the NDC 22
  - Conduct in the NDC 23
- সাইবার নিরাপত্তায় ওয়েব ব্রাউজার ব্যবহারে সতর্কতা ও করণীয় 25
- Cloud Security Maturity Model (CSMM) Diagnostic Report 28

Introduction 28
Understanding Your Cloud Maturity Report 28
Domains Maturity 29
All Factors Performance 30
Cyber Sensors Unit 45
Benefits 45
Services 45
Risk Assessment Unit 46
Incident Handling Unit 47
Benefits 47
IT AUDIT Unit 49
Payment Terms 50

WHO WE ARE

This 21st century has explored that cyber communication is one of the important vectors in globalization. As our country has already stepped towards Developing Country (DC) from Least Developed Country (LDC), we have increased using cyber communication with various important data. Our nation's growing economy has already been acknowledged by the world leaders. Nonetheless, we have also attracted many cyber criminals for the last few years. In 2016, **BGD e-GOV CIRT** (Bangladesh e-Government Computer Incident Response Team) was formed to manage Cyber Security in Bangladesh Government e-Government Network and related infrastructure with highest expertise to aware, prevent and/or investigate cyber vulnerabilities, threats and/or attacks. **BGD e-GOV CIRT** mission is to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh. We are also known as National CIRT (N-CIRT) of Bangladesh.

This is imperative to state that we have formed with the nation's best experts to manage cyber security in Bangladesh government's e-Government network and related infrastructure. Followed by ensuring scalable services by serving as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises etc.) among various stakeholders. With these visionary steps on holistic cyber incident response services, we are giving efforts to establish national cyber security incident management capabilities in Bangladesh. At the end, we would like to include that we want to place our footprint from small cyber threats to severe cyber-attacks prevention.

BGD e-GOV CIRT Services

In the cyber security world, this has been denoted that security controls are three kinds; a) Detective, b) Corrective and c) Preventive. BGD e-GOV CIRT introduces its services in two patterns in alignment with above security controls.

CIRT Services are,

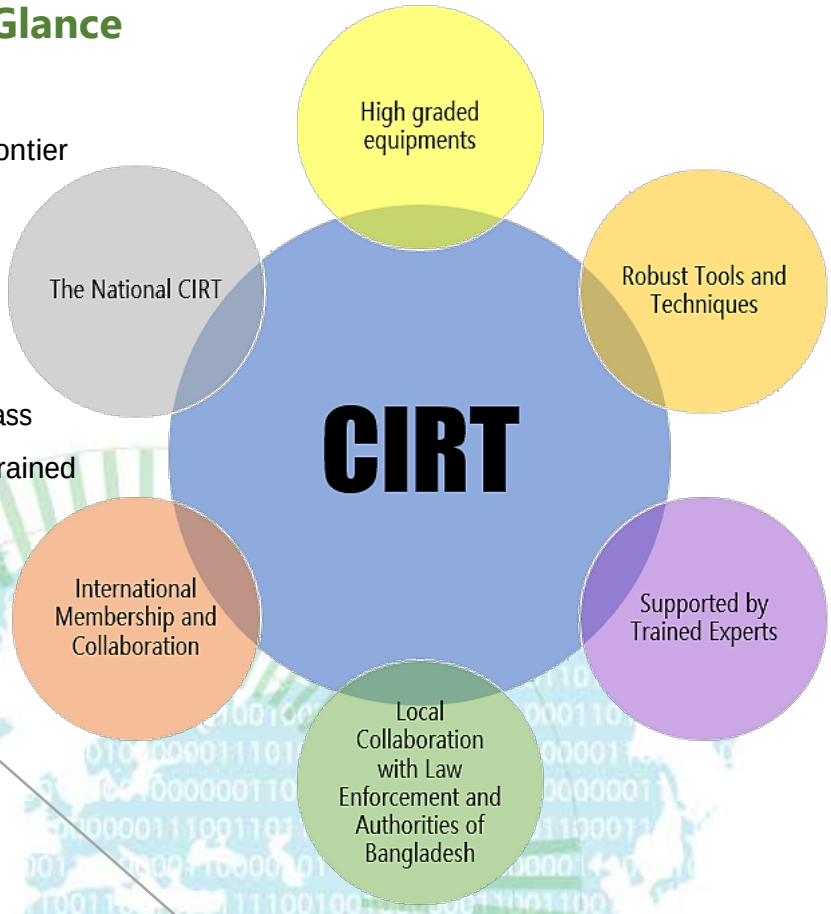
- **Proactive Services**
  - Security assessments
  - Configuration and maintenance services of security tools, applications and infrastructures
  - Intrusion detection
  - Security consulting
  - Awareness building
  - Cyber Sensor
- **Reactive Services**
  - Cyber security incident handling
    - Vulnerability Assessment
    - Penetration Test
    - Incident Analysis
    - Security Threat Notification
    - Incident Coordination
  - Digital Forensic Lab
    - Evidence Detection
    - Evidence Acquisition
    - Evidence Analysis/ Examination
    - Documenting and Reporting

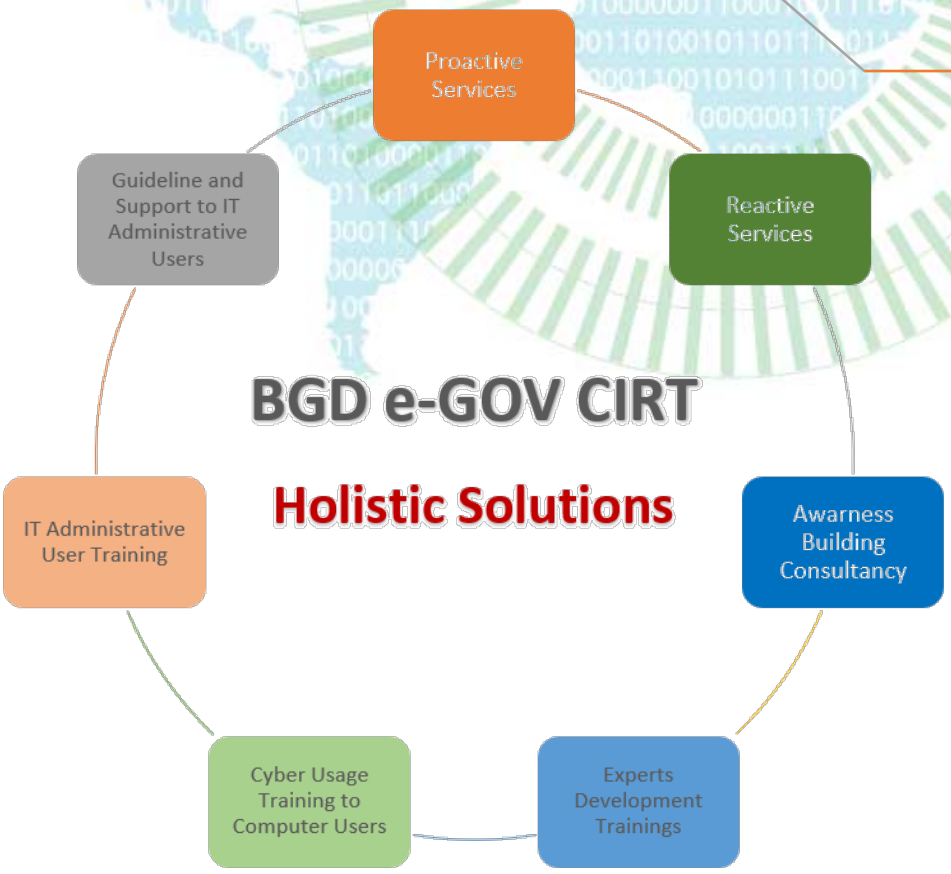
BGD e-GOV CIRT Membership

Towards BGD e-GOV CIRT's focus on spontaneous effort for cyber security prevention, its diligence has attained many international memberships. Few of the Memberships have been mentioned here. These Memberships have given BGD e-GOV CIRT enormous opportunities to attune with global movements on cyber threats and measures.

BGD e-GOV CIRT At-A-Glance

BGD e-GOV CIRT is the national frontier between Cyber Threats and Measures; where the organization is acquaintances with high graded threat prevention equipment, robust tools & techniques, world-class Policies and Measures, highly trained experts and more.

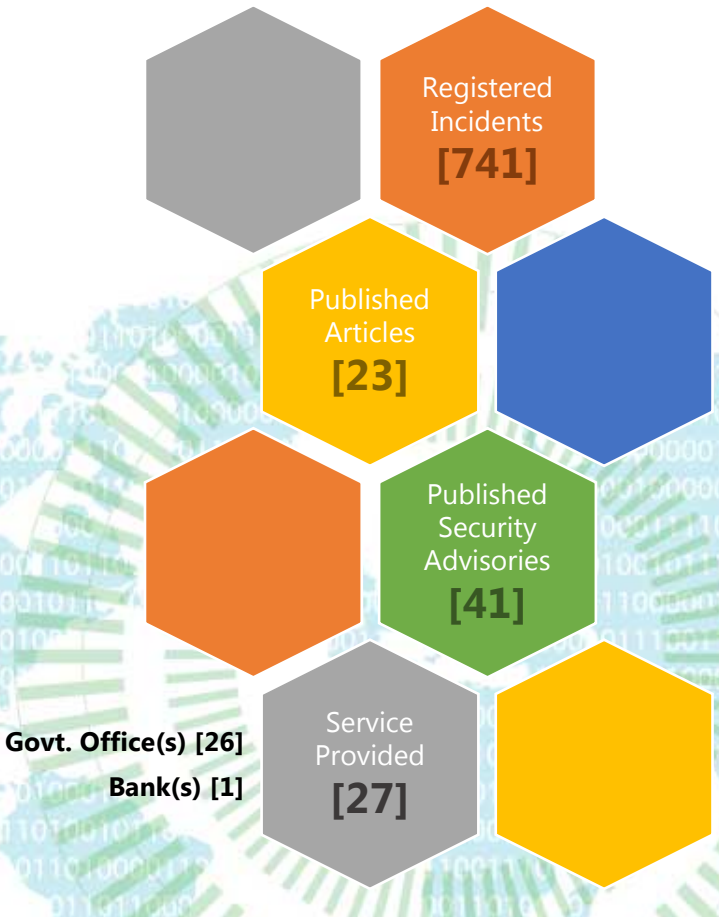




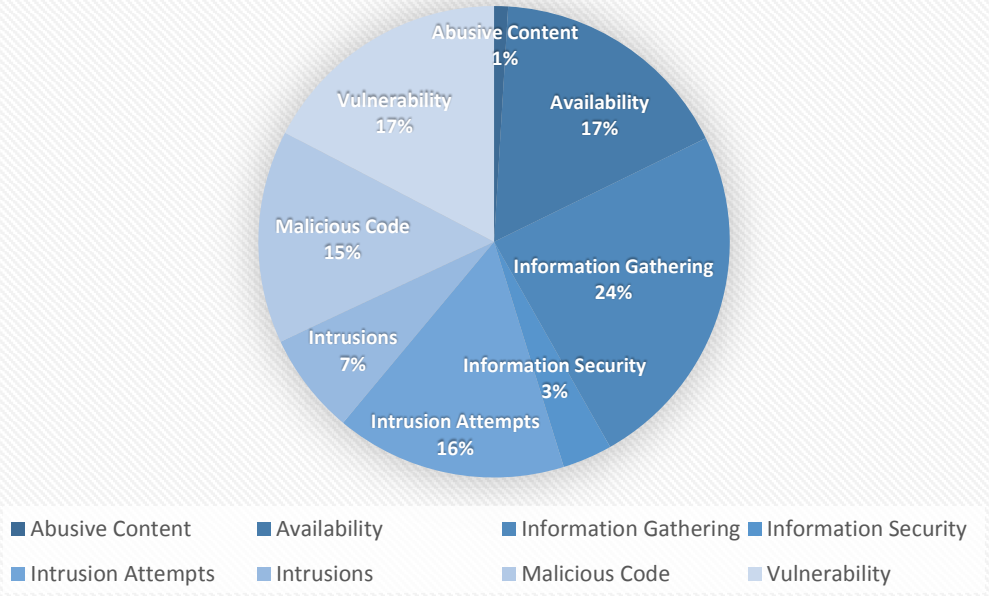
BGD e-GOV CIRT has its services and consultancy to provide holistic solutions on Cyber Security in Governmental institutes to Private sectors. Its Proactive and Reactive Services, awareness building consultancy followed by its upcoming solutions to enhance and enrich cyber security measures, will give substantial support in Government and Private sectors.

BGD e-GOV CIRT Insights

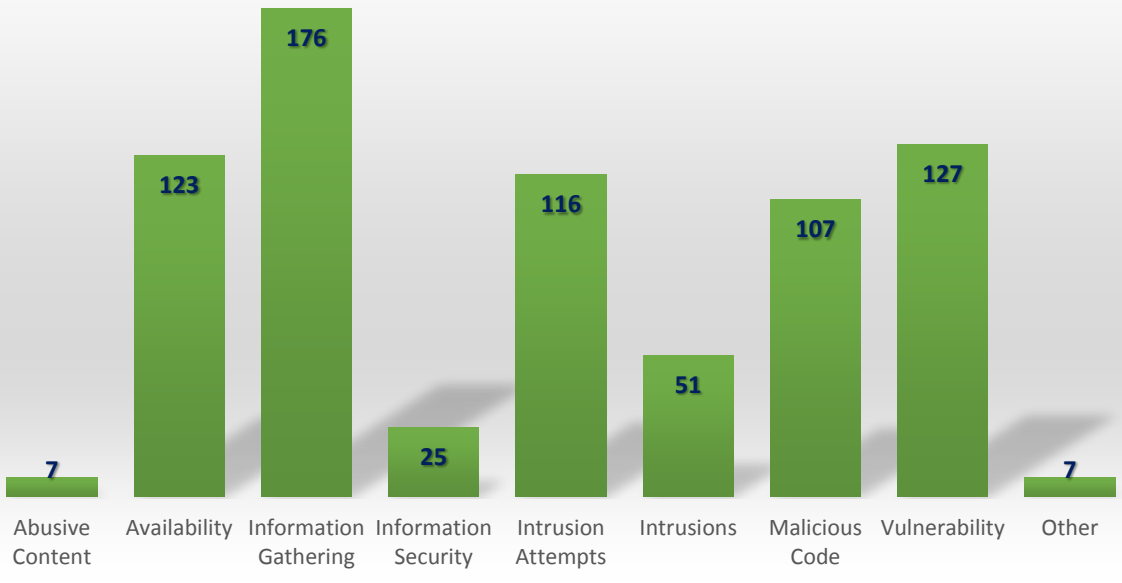
January – July, 2020



INCIDENT CLASSIFICATION

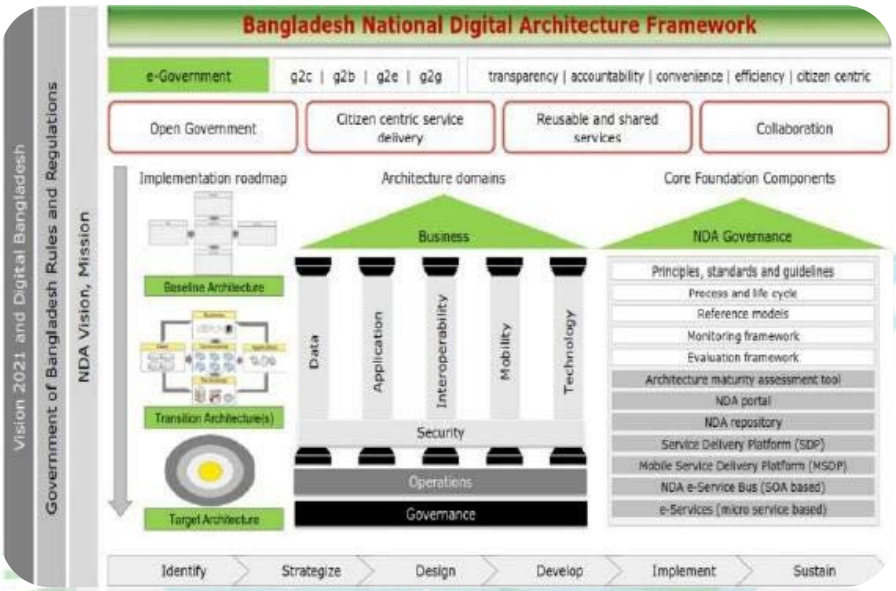


REGISTERED INCIDENTS IN NUMBER



BGD e-GOV CIRT Other Services

Bangladesh National Digital Architecture (BNDA)



The Bangladesh National Digital Architecture (BNDA) envisions to deliver a connected, integrated and governed enterprise. It is a practice that intends to strategically plan to integrate fragmented government units to enable them deliver best in class digital services. BNDA also plans to govern the digital service delivery to ensure appropriate standards are adhered, so that necessary integration, security and other aspects can be achieved seamlessly.

BNDA Components

- Architecture Repository – Comprising of frameworks, reference models, Future State Views of Government entities Bangladesh National Digital Architecture (BNDA).

- Standards – Comprising of various standards on data, business, security, etc. along with principles, guidelines and best practices.

- BNDA Digital Service (G2C, G2E and G2G) – Digital systems to transform lives of the people of Bangladesh.

- BNDA Services – Architecture compliance review service, guidance and emerging technology innovation services.

BNDA Digital Services

- e-Recruitment System
- GeoDASH platform
- Blockchain platform
- Digital Service book System
- e-Pension System
- Food Procurement System
- Project Tracking System
- BOESL Apps
- BOESL HRM Application

Global Awards & Recognitions

- Open Group President Award-2018 & 2019
- WSIS Prize 2019- ITU
- Open Group Award of Distinction- 2019
- Finalist - Enterprise Blockchain Award

e-Recruitment System

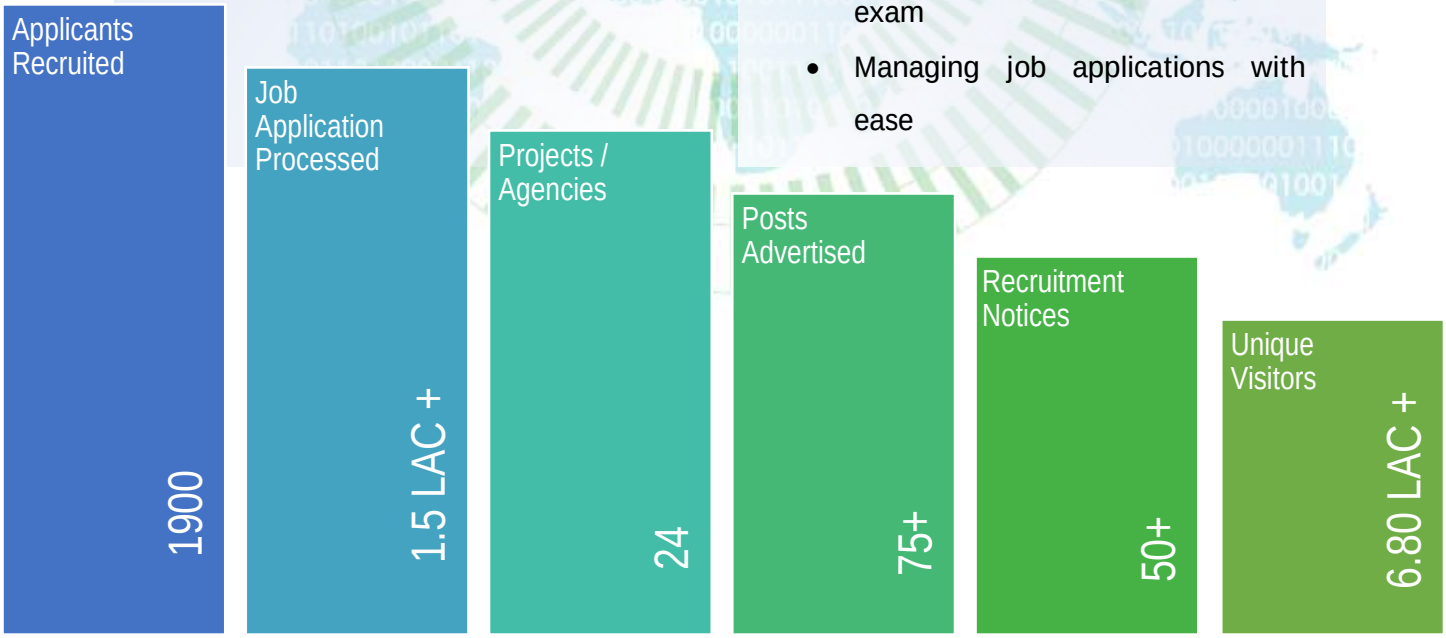
A secured web based platform to process govt. agencies' job applications digitally. It enables applicants to apply from anywhere from digital devices. Employers can process job applications and shortlist applicants. It has online exam system with automated result processing facility. A large question bank ensures managing assessment test with quality. It utilizes BlockChain technology to prevent fraudulent practices related to recruitment exam.

Features

- Registration (One time only)
- Publish recruitment Notice
- Apply for job
- Update payment information
- Prepare the list of applicants
- Prepare/send Admit Card
- Attendance sheet
- Candidate Selection
- National ID (NID) verification

Benefits

- Decrease hassles of applicants/ students for Job Application
- Reduce time of Job applications processing for employer
- Increase Exam management quality
- Uniqueness of questions is ensured
- Multiple sets of questions for same exam
- Provision for Secure starting of any exam
- Managing job applications with ease



THE Open GROUP

Open Group President's Award 2019

Food Grain Procurement System (FPS)

Food Grain Procurement System is a web Based application software to manage & control food grain procurement activities from internal market. Main Stakeholders are Farmers, Millers, Upazilla Agriculture Officer, CSD/LSD (Central Storage Depot/ Local Storage Depot), Department of Agriculture Extension (DAE) and DG Food Office. DAE and DGF are service owner, BCC is facilitating service development & maintenance.

Features

- Management of Crop procurement
- activities
- Capture Procurement Target (Upazilla Wise)
- Notification to farmer via web/sms
- Real-time dash board for stakeholders
- Various reports
- Integrated with national e-service bus

Benefits

- Decrease hassles of applicants/ students for Job Application
- Management of Crop procurement activities
- Reduce hassles of Farmers to supply paddy
- SMS notification for farmers on different occasion
- Facilitate decision making process when the season is ongoing
- Complete visibility for DAE and DG Food office over system activities

1.35 Lac+	16
• Registered Farmers	• Piloting Upazillas

অনিরাপদ ই-মেইল থেকে কিভাবে সুরক্ষিত থাকবেন

সূচনা

হ্যাকার, সাইবার অপরাধী এবং অন্যান্য অনলাইন দুষ্কৃতীদের জন্য ই-মেইল, সাইবার আক্রমণের একটি বিশেষ হাতিয়ার। বর্তমানে বেশির ভাগ সংস্থাগুলো যোগাযোগের প্রাথমিক মাধ্যম হিসাবে ই-মেইল ব্যবহার করে। সংস্থাগুলো অজ্ঞাতসারে তথ্য লঙ্ঘনের (data breaches) শিকার হতে পারে যদি তাদের কোন কর্মী অনিচ্ছাকৃত ভাবে ই-মেইলের কোন অনিরাপদ সংযুক্তি (attachment) ডাউন লোড করেন বা বা দূষিত লিঙ্ক (link) ক্লিক করেন। ব্যবহারকারীরা প্রতিদিন অসংখ্য ই-মেইল পান যাতে কিছু স্প্যাম ই-মেইল থাকে। ব্যবহারকারী যদি জিমেইল, ইয়াহু বা হটমেইল এর মত প্রধান সেবাদানকারী প্রতিষ্ঠান গুলোর ই-মেইল ব্যবহার করেন তাহলে ক্ষতিকারক

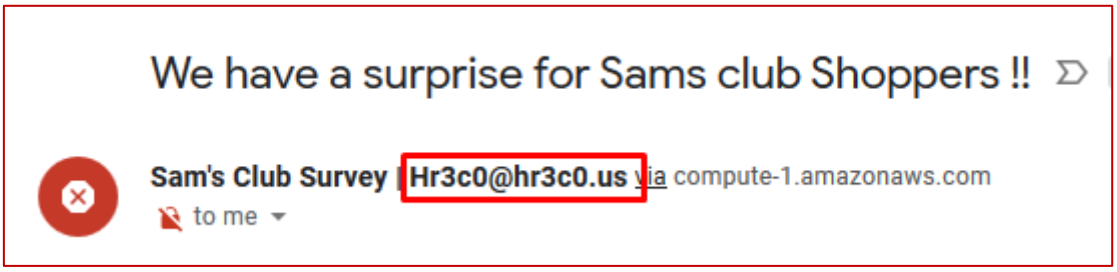
মেইলগুলোর প্রায় সবই তারা স্প্যাম হিসেবে চিহ্নিত করে। কিন্তু অফিস ই-মেইল গুলো অনেক ক্ষেত্রেই সঠিক ভাবে স্প্যাম সনাক্ত করতে পারে না। তাই সন্দেহজনক ই-মেইল খোলার ক্ষেত্রে, বিশেষত যখন তাতে কোন সংযুক্তি বা লিঙ্ক থাকে আমাদের বিশেষ খেয়াল রাখা উচিত। সন্দেহজনক ই-মেইল দ্রুত এবং সহজে চিহ্নিত করা যায় সে সম্পর্কে কিছু উপায় শেয়ার করতে যাচ্ছি।

ই-মেইল ঠিকানা ও ই-মেইলের বিষয়বস্তু লক্ষ্য করুন

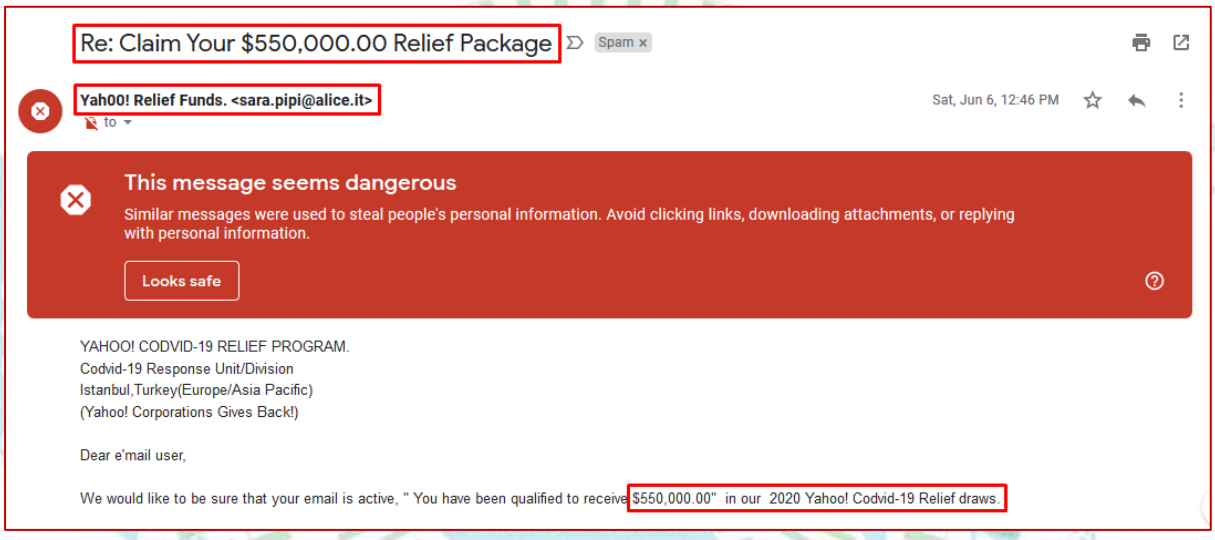
অজানা বা অদ্ভুত ঠিকানা (spoofed email addresses) থেকে আসা ই-মেইল গুলো বিশেষ ভাবে লক্ষ্য করুন। এসব ই-মেইলের প্রেরকের নাম ও ই-মেইল ঠিকানা খেয়াল করুন। উদাহরণস্বরূপ: ব্যবহারকারীর ব্যাংকের ই-মেইল ঠিকানা customers@xyzbank.com এর পরিবর্তে একজন হ্যাকার customers@xyzbank.co থেকে ই-মেইল প্রেরণ করতে পারে।

স্ক্যামাররা সাধারণত লোভনীয় বিজ্ঞাপন দিয়ে এসব ই-মেইল পাঠায়। উদাহরণস্বরূপঃ "এখনই কিনুন, সীমিত সরবরাহ, বিশাল পুরষ্কার ইত্যাদি।" ব্যবহারকারী কোন উদ্বেগ ছাড়াই ই-মেইলটি পড়তে পারবেন তবে এ জাতীয় ই-মেইলের সাথে থাকা লিঙ্ক ও সংযুক্তি পরিহার করুন।

নিচের উদাহরণ দুটি লক্ষ্য করুন:



উদাহরণ-১: অদ্ভুত ঠিকানা (email address) ব্যবহার করা হয়েছে।



উদাহরণ-২: করোনা ভাইরাসকে পুঁজি করে বিশাল অঙ্কের পুরষ্কারের কথা বলা হয়েছে।

আক্রমণকারী অনেক সময় এমন সব ই-মেইলের ঠিকানা ব্যবহার করে যা দেখতে পরিচিত বা বৈধ মনে হবে। যাদের সাথে ব্যবহারকারী প্রায়ই যোগাযোগ করেন এরকম ঠিকানা থেকেও ফিশিং ই-মেইল পেতে পারেন।

সেক্ষেত্রে বানান, বিরামচিহ্ন এবং ব্যাকরণগত ত্রুটি লক্ষ্য করুন। স্প্যাম কিংবা ফিশিং ই-মেইল গুলোতে ব্যবহারকারীর নাম ব্যবহার করার সম্ভাবনা কম থাকে। এগুলোতে "প্রিয় স্যার বা ম্যাডাম" বলে আপনাকে সম্বোধন করা হয়।

পরিশেষে, এটি বলার অপেক্ষা রাখে না যে অযৌক্তিক ঠিকানা থেকে একটি ই-মেইল (উদাহরণস্বরূপঃ xyz৩৪q@hotmail.com) অবশ্যই এমন কিছু যা ব্যবহারকারীর খোলা উচিত নয়। অবিলম্বে এটিকে স্প্যাম হিসাবে চিহ্নিত করুন এবং এটি ইন-বক্স থেকে সরিয়ে দিন।

সন্দেহজনক ই-মেইল এর সংযুক্তি ও লিঙ্ক এড়িয়ে চলুন

সবচেয়ে ভালো উপায় হল অযাচিত বা সন্দেহজনক ই-মেইল এর সংযুক্ত ফাইলটি ডাউন লোড না করা এবং লিঙ্ক ক্লিক করা থেকে বিরত থাকা। এই সব সংযুক্তিতে বিভিন্ন ম্যালওয়্যার এবং ট্রোজান (Trojan) থাকতে পারে যা দিয়ে সাইবার অপরাধীরা ব্যবহারকারীর কম্পিউটারের নিয়ন্ত্রণ নিতে, ব্যবহারকারীর কীস্ট্রোক গুলো লগ নিতে বা ব্যবহারকারীর ব্যক্তিগত / অফিসিয়াল তথ্য এবং আর্থিক ডেটা সংগ্রহ করতে পারে। লিঙ্ক এ ক্লিক করে ব্যবহারকারী ফিশিং (Phishing) এর শিকার হতে পারেন।

চিত্রঃ ফিশিং (Phishing)

ফিশিংয়ের উদাহরণ হল: এই ই-মেইলগুলো এমনভাবে প্রদর্শিত হয় যেন তারা ফেডেক্স (FedEx) এবং ডিএইচএল (DHL) এর মতো সংস্থাগুলো থেকে আসে। তাদের দেয়া লিঙ্ক ক্লিকের মাধ্যমে ব্যবহারকারীর প্যাকেজটি ট্র্যাক করতে পারবেন কিংবা লিঙ্কটি কোনও নকল সাইটে যেতে পারে যেখানে ব্যক্তিগত তথ্য সরবরাহ করতে বলা হবে।

এখন প্রশ্ন হল বিশ্বস্ত কারো কাছ থেকে সংযুক্তি সহ ই-মেইল পেলে কি করবেন?

অনিরাপদ ই-মেইল সংযুক্তি কীভাবে সনাক্ত করবেন?

ফাইল এক্সটেনশনের দিকে লক্ষ্য করা

ফাইলের নামের এক্সটেনশন গুলো সংযুক্ত ফাইলের ধরণ নির্ধারণে সহায়তা করে। উদাহরণস্বরূপ: যদি ফাইলটির নাম abc.jpg হয় তাহলে .jpg এক্সটেনশনের মানে এটি একটি ছবি। abc.avi দিয়ে শেষ হলে এটি একটি ভিডিও ফাইল। ব্যবহারকারীর যে এক্সটেনশনটি এড়ানো উচিত তা হল .exe, যা ডাউন লোড করলে ডিভাইসে ম্যালওয়ার ইন্সটলেশন হবে। আক্রমণকারীরা এগুলো এরকম ভাবে প্রোগ্রাম করে যে

অনেক সময় এই ম্যালওয়ার গুলো অ্যান্টি-ভাইরাস এবং ই-মেইল সেবা সরবরাহকারীদের সুরক্ষা এড়িয়ে যেতে পারে।

যে এক্সটেনশন গুলো ব্যবহারকারীর এড়িয়ে যাওয়া উচিত .jar, .cpl, .bat, .msi, .js, .wsf ইত্যাদি।

JAR: They can take advantage of Java runtime insecurities.

BAT: Contains a list of commands that run in MS-DOS.

PSC১: A PowerShell script with commands.

VB and VBS: A Visual Basic script with embedded code.

MSI: Another type of Windows installer.

CMD: Similar to BAT files.

REG: Windows registry files.

WSF: A Windows Script File that permits mixed scripting languages.

চিত্র: ফাইল এক্সটেনশন

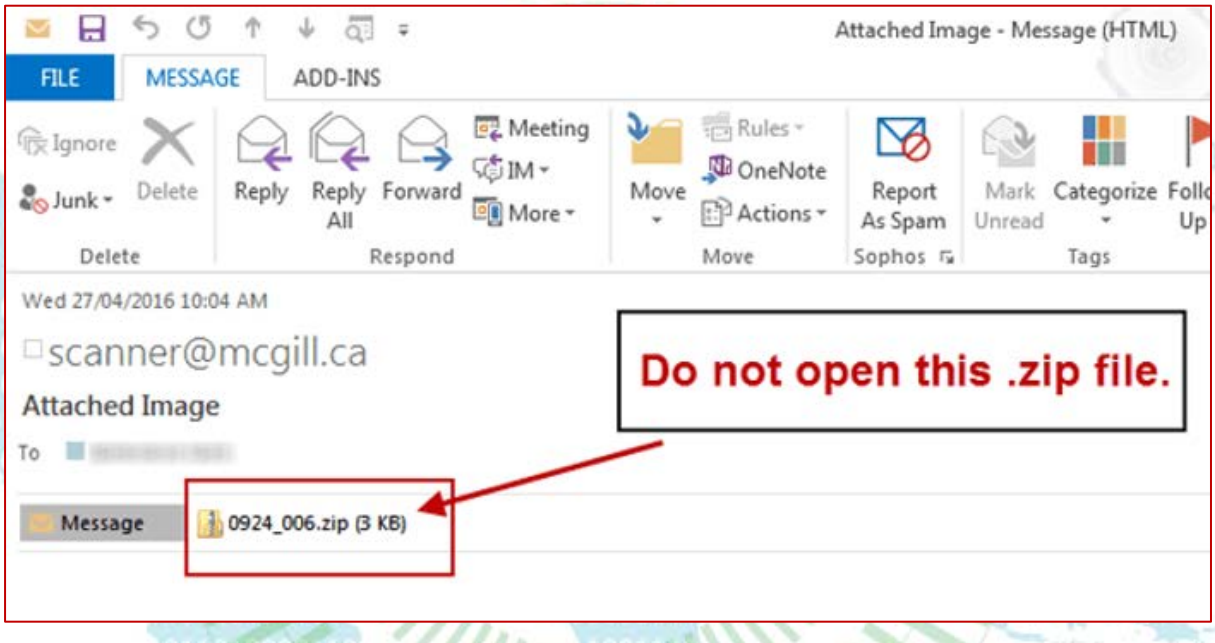
যদি এটি কেবল একটি অফিস ফাইল হয়?

এটি ভাল হওয়া উচিত, তবে ব্যবহারকারীর কিছু সতর্কতা অবলম্বন করতে হবে। আক্রমণকারী মাইক্রোসফট অফিস ফাইল দিয়েও ব্যবহারকারীর ডিভাইসকে সংক্রামিত করতে পারে। এটিতে ম্যাক্রো (macros) থাকতে পারে, যা কিছু নির্দিষ্ট কার্য সম্পাদনের নির্দেশনা। যদি অফিস ফাইলটির এক্সটেনশন m দিয়ে শেষ হয় তাহলে এটি ম্যাক্রো ফাইল। যেমন: .docm. pptm, and .xlsm ইত্যাদি। তবে কাজের প্রয়োজনে নিরাপদ ম্যাক্রো ফাইল ব্যবহার করার সময় বিশ্বস্ত উৎস থেকে যাচাই করে নিবেন।

আরেকটা প্রশ্ন আসতে পারে, যদি সংযুক্ত ফাইলগুলো আর্কাইভ বা জিপ (.৭z, .rar, or .zip) করা থাকে?

ভাইরাস স্ক্যান এড়াতে হ্যাকাররা এগুলো ব্যবহার করে কারণ তারা এতে ম্যালওয়্যার লুকিয়ে রাখতে পারে।

যদি জিপ করা সংযুক্তি সহ কোনও ই-মেইল পেয়ে থাকেন এবং এটি খোলার জন্য একটি পাসওয়ার্ড লিখতে বলে, এটি সন্দেহজনক হতে পারে। সুতরাং, এনক্রিপ্ট করা ফাইলটি খোলার আগে নিশ্চিত হয়ে নিন যে এটি বিশ্বস্ত উৎস থেকে এসেছে কিনা।



চিত্রঃ জিপ ফাইল সংযুক্ত ই-মেইল

সর্বদা সক্রিয় ও হালনাগাদ অ্যান্টি-ভাইরাস ব্যবহার করা

কোনও ই-মেইল সংযুক্তির সম্ভাব্য সুরক্ষা সম্পর্কে ব্যবহারকারী যদি সন্দেহ পোষণ করেন তাহলে ডাউন-লোড করার পর অ্যান্টি-ভাইরাস প্রোগ্রামটি দিয়ে যাচাই করে নিন। বলা বাহুল্য, ফাইলটি ঝুঁকিপূর্ণ হলে ব্যবহারকারীর অ্যান্টি-ভাইরাস প্রোগ্রামটি স্বয়ংক্রিয়ভাবে ফাইলটিকে ফ্ল্যাগ করবে। কম্পিউটার থেকে ফাইলটি মুছে ফেলুন এবং এটিকে পুনরায় ডাউন-লোড করবেন না। মনে রাখবেন, যদিও অ্যান্টি-ভাইরাস অ্যাপ্লিকেশনগুলো নিখুঁত নাও হতে পারে, তবে সন্দেহজনক ই-মেইল সংযুক্তি এড়িয়ে চলাই নিরাপদ।

টিপসঃ শুরুতে বলেছিলাম ব্যবহারকারী যদি জিমেইল, ইয়াহু বা হটমেইল এর মত প্রধান সেবাদানকারী প্রতিষ্ঠান গুলোর ই-মেইল ব্যবহার করেন তাহলে ক্ষতিকারক মেইলগুলোর প্রায় সবই এরা স্প্যাম হিসেবে চিহ্নিত করে। অনেক প্রতিষ্ঠানই অফিস ই-মেইল এর পাশাপাশি ব্যক্তিগত ই-মেইল ব্যবহারের অনুমতি দেয়। তাই ব্যবহারকারীর প্রাতিষ্ঠানিক ই-মেইলে আসা কোন দরকারি সংযুক্তি নিয়ে সন্দেহ থাকলে এটি ব্যবহারকারীর ব্যক্তিগত ই-মেইলে পাঠিয়ে চেক করে নিতে পারেন। এক্ষেত্রে অবশ্যই প্রাতিষ্ঠানিক বিধিনিষেধ গুলো জেনে নিবেন।

সাধারণ কিছু উপলব্ধি থেকেই একটি ই-মেইল এর সত্যতা অনুমান করা যায়। সামান্য অসতর্কতার কারণে চরমভাবে ক্ষতিগ্রস্ত হচ্ছেন অনেক ব্যবহারকারী। প্রযুক্তি ব্যবহারে সতর্কতা ও সচেতনতাই একজন ব্যবহারকারীকে সাইবার আক্রমণের শিকার হতে রক্ষা করতে পারে। তাই সতর্ক হোন, নিরাপদ থাকুন।

ছবি সূত্রঃ ইন্টারনেট ।

সাহেবুল করিম
ইন্সিডেন্ট হেল্প ডেস্ক এসোসিয়েট
বিজিডি ই-গভ সার্ট

Data Center Management Best Practices

Data Center Management is a holistic process to oversee the operational and technical issues within a data center. It includes environmental control, physical and logical security, network connectivity, hardware server and storage operations and management of the services and applications. Running a data center is a complex undertaking. In addition to maintaining the strict physical security measures and logical security protocols needed to secure data, facility personnel face an ongoing challenge of optimizing IT infrastructure to improve power efficiencies and maximize cooling capacity. Quality data center operations are a key differentiator for customers looking for the best possible partner to house and manage their IT infrastructure solutions. Data centers are more than just an investment. They are a critical resource that customers depend upon. This makes it critically important for a facility to implement a variety of management and maintenance best practices to improve its data center operations.

The very best managed data centers achieve that status because they have well documented procedures for everything. That means operations and facilities staff have a script to follow for everything they do and even for events they never encountered before. Data Center managers need to establish a culture among the data center staff that embraces and strictly adheres to the documented processes. Customers look for a data center culture that literally celebrates and compulsively adheres to process and procedure. And the first place they will find the crucial evidence that such culture exists is in the documentation, because it is the documentation that makes data center operations and facilities management standardized and repeatable, and empowers continuous improvement.

Collaboration among data center staff is essential for a well-managed data center. This must be embedded in the organizational structure as a linchpin of ongoing process and documentation evolution and a key contributor to efficiency and even disaster response. The Uptime Institute states that the separate IT and

facilities team that operate in data centers should be closely aligned that they become one "Integrated Critical Environments" (ICE) team.

For a data center to maintain consistent reliability and availability across a varied and changing footprint requires constant monitoring and maintenance of critical systems. This helps to avoid the avoidable problems. Data Centers need to have effective monitoring and maintenance strategies and processes to help protect them from unplanned outages, and reduce repairs and downtime related costs.

To well manage a data center, efficient and effective planning is necessary. It provides insights about equipment including their location, current capacities, and projected growth. That is why data center managers need to do proper planning in a timely manner so that they are able to oversee inventory, anticipate capacity needs, and prepare for new implementations. It is necessary to have well documented change management procedure, which needs to be followed strictly. Also it is necessary to get stakeholder support when implementing change to avert resistance. There must be a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP) to ensure operations in an emergency.

The importance of well-trained staff including ongoing training for efficient operation of data centers cannot be overstated. It is very important to have proper training program to train data center staff so that they always remain at the top of their game. Without continuous training of data center staff, data centers cannot increase operational efficiency and effectiveness. It is also necessary to benchmark for tracking performance of data center staff over time. Data centers need to develop security awareness curriculum and provide training to all data center staff on security to reduce vulnerability to man-made threats.

For data centers applying new technologies and honing best practice facilities design standards is an ongoing process. But the best technology and design, alone, will not deliver the efficient, high-quality data center. It takes an organization of experienced, well-trained, collaborative staff with a commitment to rigorous adherence to standards and methods, to deliver on the promise to always be up and running, come what may – to be the "Perfect Data Center".

Reference Picture: Internet

Farhad Hussain
Senior Technical Specialist (Infrastructure)
Strengthening BGD e-GOV CIRT Project

Standard Operating Procedure (SOP) of National Data Center

Purpose

This Standard Operating Procedure (SOP) will serve as guiding document to ensure smooth operations of NDC. The objective is to achieve security, efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with policies. It will clarify processes by which all current and future stakeholders of NDC shall be mandated to follow and adhere.

Scope

This SOP shall apply to all NDC staffs, government agencies, contractors, vendors, visitors and all the stakeholders who are availing NDC services. This SOP shall also cover all equipments that are located in NDC.

Introduction

NDC is a critical national ICT infrastructure, which serves as platform to efficiently and reliably deliver G2G, G2C and G2B services. It is located in ICT Tower, at Agargaon, Dhaka.

NDC Access Procedure

A. Primary Guidelines

The “National Data Center” is a restricted area required a much greater level of control than normal non-public foundation spaces. Only those individual who are expressly authorized to do so may enter this area. Access privileges will be grated to individuals who have a legitimate business need to be in the data center. Any questions regarding NDC access procedure should be addressed with the Director, NDC.

B. Role Definitions

i) NDC Staff: Employees who work at the National Data Center (NDC).

ii) Authorized Staff: All BCC and ICT Division staff, authorized to gain access to the National Data Center (NDC), but do not work at the National Data Center (NDC).

iii) Authorized Vendor: External service providers' staff, authorized to gain access to the National Data Center (NDC), through contractual arrangement and appropriate approval.

iv) Visitors: All others who may occasionally visit the National Data Center (NDC) but are authorized to be in the not National Data Center (NDC) without escort.

C. Access Authorization Levels

The National Data Center (NDC) is intended to provide a 24x7x365 high availability, secure environment for systems that need a high level of security. All personnel must have proper authorization to obtain access to the NDC. There are several levels of authorization based on the access required. All individuals must be logged when entering/exiting the NDC Center regardless of their level of authorization.

C1. Level III Authorization

Level III authorization is granted to NDC staff whose job responsibilities require that they have access to the entire area of NDC. Level III authorization provides for unassisted, unescorted access to the entire NDC on 24x7x365 basis.

C2. Level II Authorization

Level II authorization is granted to a person who does not qualify for Level III authorization but has a legitimate reason for unsupervised access to some areas of the NDC. Each NDC staff is granted Level II authorization according to their job responsibilities.

Each staff of authorized vendor is granted Level II authorization according to the nature of work and access area is determined on a case-by-case basis.

Authorized staff is also granted Level II authorization and access area is determined on a case-by-case basis.

All NDC employees must complete NDC Employee Access Form while joining as a NDC staff. This form is reviewed and approved by the NDC Manager and according to the role of NDC staff the following access authorizations are granted:

- Access to the Server room and Network room is granted to the Infrastructure, Server and Network team members.
- Access to the Power room is granted to the Infrastructure team members.
- Access to the Telecommunication room is granted to the Network team members.
- Access to the Fire safety equipment room is granted to the Infrastructure team members.

C3. Level I Authorization

Level I authorization grants escorted assistance to the NDC during normal weekday business hours (9 am - 5 pm). Entry to the Data Center will not be granted to access cards assigned to those individuals who have received Level I authorization. Level I authorized person must be escorted at all times by Level II authorized or higher personnel.

Visitors are granted Level I authorization. A person given Level I authorization to the NDC must sign in and out under the direct supervision of a person with Level II authorization or higher. A person with Level I authorization must provide positive identification upon demand, and must leave the area when requested to do so.

All Client and his representative (Service Engineers and Support Staff) entering data center for support must deposit their Mobile Phone, Camera, Bag at the counter. They will not be allowed to take these items or any personal belonging on data center floor for security.

D. Proof of Entry into the NDC

An entry register is kept at the NDC door. Everyone must log his/her details (name, address, purpose, etc.) and sign in and out mentioning entry and exit time to and from the NDC. Entries in the register are considered as proof of entry and duration of stay of any person in the NDC. No other means of proof of attendance is applicable unless so duly notified by the authority in writing.

E. Data Center Door

All doors to the NDC must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

- Allow officially approved and logged entrance and exit of authorized individuals
- Permit the transfer of supplies/equipment as directly supervised by a person with General Access to the area
- Prop open a door to the NDC only if it is necessary to increase airflow into the Data Center in the case on an air conditioning failure. In this case, staff personnel with Level II or higher authorization must be present and limit access to the Data Center.

F. Exception Reporting

All infractions of the NDC Access Procedure shall be reported to the Director, NDC. Individuals with Level II or higher authorization to the NDC are to monitor the area and remove any individual who appears to be compromising either the security of the NDC or its activities, or who is disrupting operation. It is particularly important that individuals with Level II or higher authorization show initiative in monitoring and maintaining the security of the NDC.

Approval Procedure of Service Requests

All service requests received by the NDC staff must follow the following approval process:

A. Services with no financial involvement

If a service request is received, which has no financial involvement then the initiating staff of the said service needs to obtain approval from his/her supervisor/manager before fulfillment of the service request.

B. Services with financial involvement

If a service request is received, which has financial involvement then the initiating staff of the said service will forward the service request to his/her supervisor/manager.

The supervisor/manager will forward the service request with details to the director, NDC for approval.

The director, NDC will decide whether to forward the service request for approval of higher authority.

Equipment in the NDC

The NDC is intended as a limited physical access location for computer systems. Individuals who administer equipment that is housed in the NDC should plan to have physical access to their systems to perform hardware modification, repair, or replacement only. With this in mind, all servers should be configured with secure access administrative tools to allow for as much remote administration as possible. Only if such tools are not available or feasible, will physical access to the Data Center be allowed.

A. Equipment Installation

- The Equipment Installation Form must be completed for all equipment to be placed in the NDC. NDC manager will deny entry to authorized staff or vendors who intend to install or change equipment without a properly completed form.
- Equipment housed in the NDC must meet certain system specifications. These include:
  - All new equipment must be rack mountable unless prior arrangements have been made to allow a particular non rack-mountable piece of equipment into the room.
  - Equipment that has a business need to be in the room and is currently not rack mountable should be replaced with rack mountable units. If this is not possible, the functions the equipment provides should be relocated to hardware more appropriate for the NDC.
  - All equipment should contain dual power supplies (redundant), unless an exception is made by the NDC Manager.
  - All rack mounted power distribution units must be connected to the NDC UPS backed power grid, and must provide remote monitoring capability to the monitoring systems.

- No stand-alone or rack mount UPS units will be allowed.
- Placement of new systems and hardware in the NDC must be coordinated with the NDC Manager and/or NDC Technical Team.
- As the number of systems housed in the NDC grows, the infrastructure that supports the NDC must be expanded. This may mean a delay in the deployment of hardware into the NDC until the appropriate infrastructure (including console, network, power and rack space) is in place.

B. Equipment Removal

The Equipment Removal Form must be completed for all equipment to be removed from the NDC. NDC manager will deny entry to authorized staff or vendors who intend to remove equipment without a properly completed form.

Conduct in the NDC

In order to ensure that the systems housed within the NDC are kept secure, the following policies apply to all personnel requiring access:

- All personnel who access the Data Center must have proper authorization. Individuals without proper authorization may be denied access at any time for any reason.
- All authorized personnel must be logged in and out when visiting the NDC to document the time and purpose of their visit.
- Authorized personnel shall only access equipment for which they are responsible. If any person accesses equipment for which they are not responsible, their NDC access privileges may be downgraded or revoked.
- Only members of the NDC Technical Team shall access the sub-floor or remove a floor tile.
- Visitors to the NDC must adhere to the visitor guidelines
- Food and drink are not allowed in the NDC.
- No hazardous materials are allowed within the NDC.
- No cleaning supplies or any other liquid are allowed within the NDC without prior approval.

- No cutting of any material (pipes, floor tiles, etc.) shall be performed inside the NDC unless special arrangements are made.
- All packing material must be removed from computer equipment/components in the designated staging areas before being moved into the server area.
- In the event of an emergency contact the NDC Manager immediately.

Approved By:

Tarique M Barkatullah
Director (National Data Center)
Bangladesh Computer Council
ICT Division

সাইবার নিরাপত্তায় ওয়েব ব্রাউজার ব্যবহারে সতর্কতা ও করণীয়

তথ্যপ্রযুক্তির এই ক্রমবর্ধমান উন্নতি, প্রচার, প্রসার ও ব্যবহারের যুগে মানুষের কাছে বিভিন্ন ধরণের তথ্য এবং সেবা পৌছে দেওয়ার সহজ মাধ্যম হচ্ছে ইন্টারনেট। এই ইন্টারনেট ব্যবহার করে মানুষ ঘরে বসে পড়াশোনা থেকে শুরু করে পণ্য ক্রয় বিক্রয়, ব্যবসা বানিজ্য পরিচালনা, ভিডিও কলে কথা বলা, বাসার ইউটিলিটি (বিদ্যুত, পানি, গ্যাস) বিল পরিশোধ করা, এমনকি দৈনন্দিনের কাঁচাবাজার পন্য সামগ্রী ক্রয় করতে পারছেন।

ইন্টারনেটের মাধ্যমে তথ্য ও সেবা পাওয়ার জন্য বর্তমানে বিভিন্ন অ্যাপ্লিকেশন থাকলেও সবচেয়ে বেশি ব্যবহৃত হয় ওয়েব ব্রাউজার, যা প্রায় প্রত্যেক কম্পিউটার এ অপারেটিং সিস্টেমের সাথে ইন্সটল্ড (Installed) থাকে। বিভিন্ন ধরনের ওয়েব ব্রাউজার থাকলেও বহুল ব্যবহৃত ও উল্লেখযোগ্য হচ্ছে মজিলা ফায়ারফক্স (Mozilla Firefox), গুগল ক্রোম (Google Chrome), অ্যাপল সাফারি (Apple Safari), অপেরা (Opera), ইন্টারনেট এক্সপ্লোরার (Internet Explorer) ইত্যাদি।

ইন্টারনেট ভিত্তিক তথ্য ও সেবা পাওয়ার জন্য যেহেতু ওয়েব ব্রাউজার অধিক ব্যবহার করা হয় তাই ওয়েব ব্রাউজার এর নিরাপত্তা নিশ্চিত করা এবং নিরাপদে ব্যবহার করা অতি জরুরী। কম্পিউটার এর অপারেটিং সিস্টেমের সাথে যে ওয়েব ব্রাউজার গতানুগতিকভাবে দেয়া থাকে অথবা আমরা যে ওয়েব ব্রাউজার ইনস্টল (Install) করি, সাধারণত তাতে নিরাপত্তা নিশ্চিত করা থাকে না।

ইন্টারনেট ব্যবহারকারীর সাইবার নিরাপত্তা বিষয়ক পর্যাপ্ত জ্ঞান না থাকলে এবং ওয়েব ব্রাউজার এর নিরাপত্তা নিশ্চিত করা না হলে, খুব সহজেই ইন্টারনেটে ছড়িয়ে থাকা বিভিন্ন ধরণের ভাইরাস, ম্যালওয়্যার বা অন্যান্য ক্ষতিকর প্রোগ্রাম, ব্যবহারকারীর অগোচরে তার কম্পিউটার এ অনুপ্রবেশ করতে পারে এবং এর মাধ্যমে সাইবার অপরাধীরা ব্যবহারকারীর কম্পিউটার এর সম্পূর্ণ নিয়ন্ত্রণ নিতে সক্ষম হতে পারে।

ওয়েব ব্রাউজার এর নিরাপত্তা নিশ্চিত করার জন্য কিছু করণীয় নিম্নে আলোচনা করা হলো।

১) প্রতিটি ওয়েব ব্রাউজার এ প্রাইভেসি সেটিংস থাকে। ব্যবহারকারীকে এই সেটিংসগুলো ভালো করে পর্যালোচনা করে কনফিগার (Configure) করা যাতে করে ব্রাউজার এর নিরাপত্তা বিঘ্নিত না হয়।

২) সবসময় ওয়েব ব্রাউজার হালনাগাদ (Update) রাখা।

৩) ওয়েব ব্রাউজার এর প্লাগ-ইনস (Plug-ins), অ্যাডঅনস (Add-ons) এবং এক্সটেনশনস (Extensions) ডাউনলোড করার সময় সচেতন থাকতে হবে যাতে ক্ষতিকর প্লাগ-ইনস, অ্যাডঅনস বা এক্সটেনশনস ইনস্টল না হয়ে যায়।

৪) ব্যবহৃত প্লাগ-ইনস সমূহ হালনাগাদ রাখা এবং অব্যবহৃত ও অপ্রয়োজনীয় প্লাগ-ইনস আনইনস্টল (Uninstall) করা।

৫) সর্বদা সক্রিয় ও হালনাগাদ অ্যান্টি-ভাইরাস ব্যবহার করা।

৬) বিভিন্ন ধরনের ওয়েব ব্রাউজার সিকিউরিটি প্লাগ-ইনস ব্যবহার করা এবং অপ্রত্যাশিত পপআপ (popup) বাধা প্রদানকারী এক্সটেনশনস (Extensions) ব্যবহার করা। যেমন, এ্যডব্লক প্লাস (Adblock Plus) এক্সটেনশন।

৭) ৩২-বিট প্রোগ্রাম এর চাইতে ৬৪-বিট প্রোগ্রাম এর নিরাপত্তা ব্যবস্থা উন্নত হওয়ায় ৬৪-বিট এর ওয়েব ব্রাউজার ব্যবহার করা।

সাইবার আক্রমন থেকে বাঁচার জন্য ওয়েব ব্রাউজার ব্যবহারকারীর জন্য কিছু সতর্কতা আলোচনা করা হলো।

১) ওয়েব ব্রাউজার এ কখনোই পাসওয়ার্ড সংরক্ষণ করা ঠিক নয় কারণ যদি ব্যবহারকারীর কম্পিউটার কখনো ভাইরাস, ম্যালওয়্যার বা অন্যান্য ক্ষতিকর প্রোগ্রাম দ্বারা আক্রান্ত হয় তাহলে সাইবার অপরাধী যে কোন সময় সেই পাসওয়ার্ড পেতে পারে। এক্ষেত্রে পাসওয়ার্ড সংরক্ষণ করার জন্য ব্যবহারকারী নিরাপদ কোন সফটওয়্যার ব্যবহার করতে পারেন যেমন, কীপাস পাসওয়ার্ড সেফ (KeePass Password Safe)

২) ওয়েব ব্রাউজার এর ব্রাউজিং হিস্টোরি (Browsing history) এবং ক্যাশ (Cache) মুছে ফেলা।

৩) ওয়েব ব্রাউজার এর অটোফিল (Autofill) সুবিধা নিষ্ক্রিয় রাখা যাতে করে ওয়েব ব্রাউজার এ ব্যবহারকারীর কোন তথ্য সংরক্ষিত না থাকে।

৪) ব্যবহারকারী যদি সাইবার ক্যাফে বা অন্যের কোন কম্পিউটারের ওয়েব ব্রাউজার মাধ্যমে ইন্টারনেট ব্যবহার করে তবে ওয়েব ব্রাউজার এর ইনকগনিটো মোড (Incognito mode) ব্যবহার করা যাতে করে ব্যবহারকারীর কোন তথ্য ওয়েব ব্রাউজার এ সংরক্ষিত না থাকে।

সকলের সাবধানতা এবং সচেতনতাই পারে নিরাপদ সাইবার পরিবেশ তৈরী করতে।

ছবি সূত্রঃ ইন্টারনেট ।

মোহাম্মদ আরিফুল ইসলাম
ইনফরমেশন সিকিউরিটি স্পেশালিষ্ট
বিজিডি ই-গভ সার্ট

Cloud Security Maturity Model (CSMM) Diagnostic Report

Introduction

Both team have co-developed the Cloud Security Maturity Model (CSMM) to help organizations understand the maturity of their current cloud security practices across 12 categories over 3 domains. BGD e-GOV CIRT partnering with Cloud Security Alliance to integrate the CSMM into their cloud security research program as well as their certification and training initiatives. The diagnostic is meant to help organizations understand what their cloud security journey looks like, and more importantly, to be able to consciously determine how mature they want to be for each category.

Understanding Your Cloud Maturity Report

The CSMM is a set of guidelines, not all of which will work for every organization. Organizations should use the model as a starting point and a means to make decisions about how much investment in each category makes sense for their environment. To help gain value from this report, here we detail the 3 domains and their role in helping increase the maturity of your cloud security program:

Foundational Domains

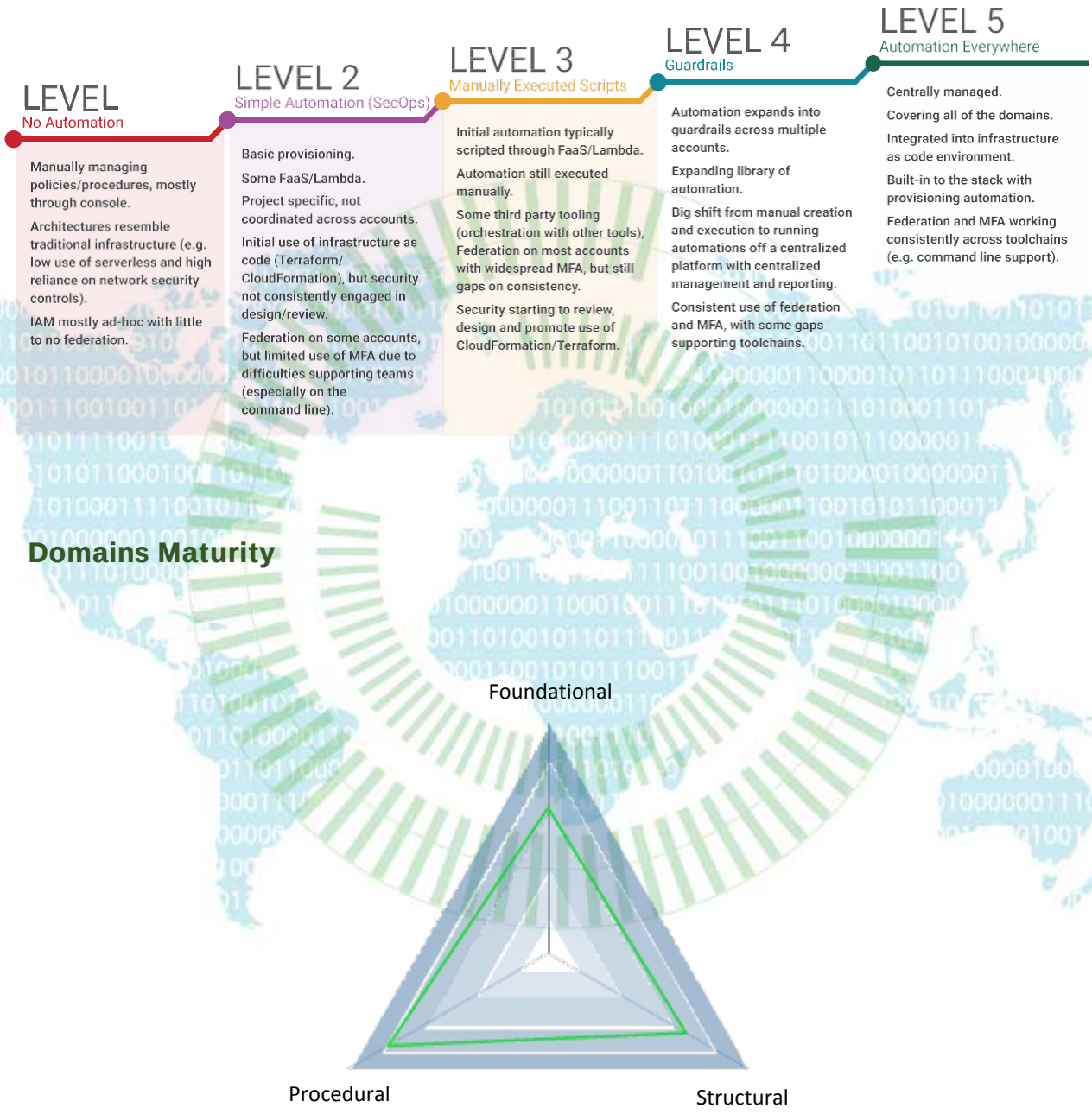
Represents the core, critical domains that ensure a secure baseline on which to build your cloud security environment. This is where you start laying the foundation for a strong cloud security program.

Structural Domains

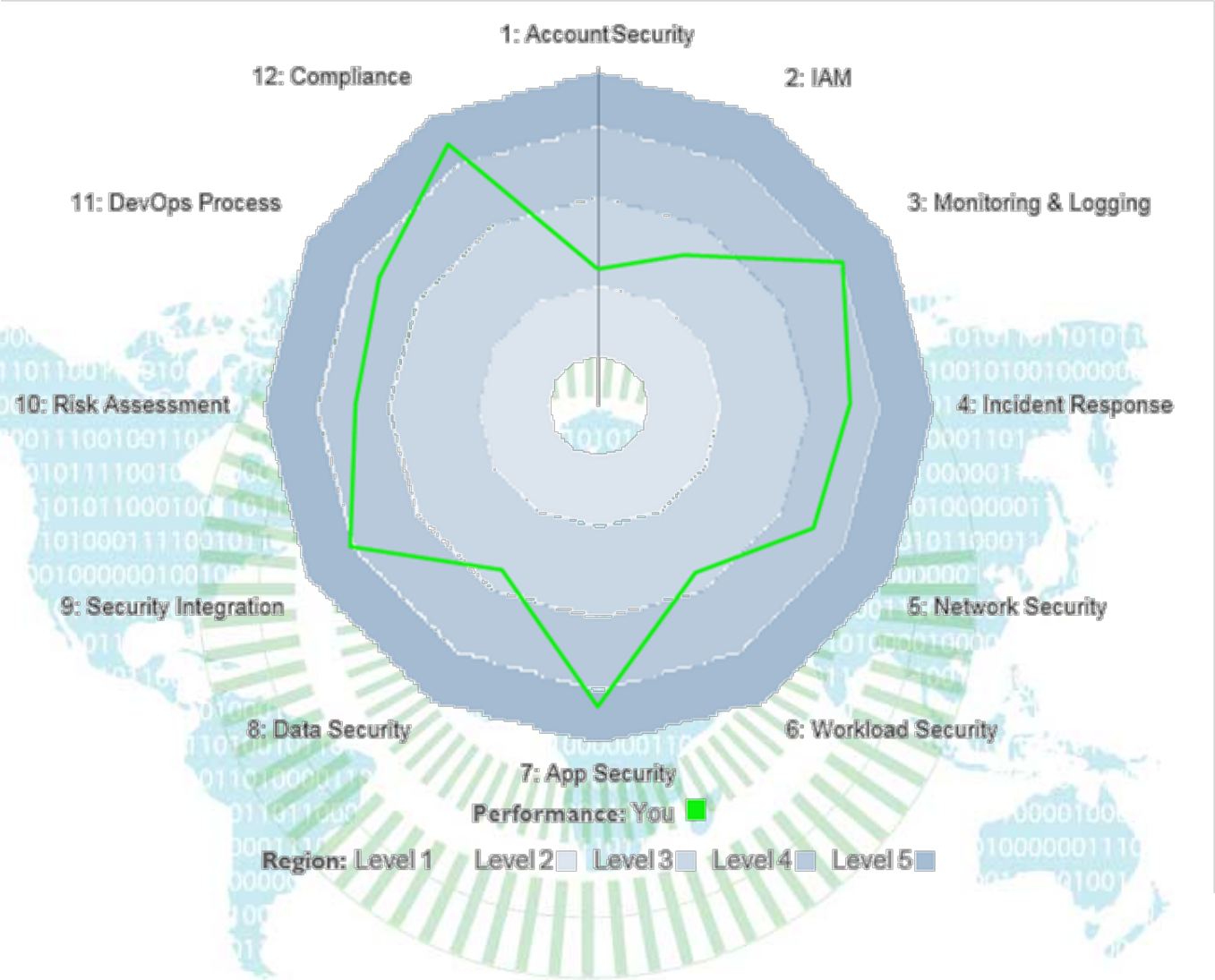
Represents what would traditionally be considered security and become the building blocks of your cloud security program. This domain is about understanding the differences in how the technology of securing resources works and leveraging both automation and orchestration to enable all of the requisite controls to work in an agile, adaptive manner.

Procedural Domains

Represents many of the fundamental process and procedural changes required to protect your cloud environment(s) reliably and consistently. Each category highlights how the cloud is different than traditional datacenters and what you must do to embrace those differences.



All Factors Performance



Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Compute				
Virtual servers	Elastic Compute Cloud (EC2) Instances	Azure Virtual Machines	Compute Engine	Virtual servers allow users to deploy, manage and maintain OS and server software; instance types provide combinations of CPU/RAM; users pay for what they use with the flexibility to change sizes
	Amazon Lightsail	Azure Virtual Machines and Images	–	Collection of virtual machine templates to select from when building out your virtual machine
Container instances	EC2 Container Service (ECS)	Azure Container Service	Container / Kubernetes Engine	Provides clustering and an orchestration layer for controlling the deployment of containers onto hosts and the management of the containers within a cluster
	EC2 Container Registry	Azure Container Registry	Container Registry	Repository service for storing container images that is used to create different types of container deployments
Microservices / container orchestrators	Elastic Container Service for Kubernetes (EKS)	Azure Container Service (AKS)	–	Deploy orchestrated containerized applications with Kubernetes that simplify monitoring and cluster management through auto upgrades and a built-in operations console

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Compute (Continued)				
Serverless	Lambda	Azure Functions Azure Event Grid Web Jobs	Cloud Functions	Enables users to integrate systems and run backend processes in response to events or schedules without provisioning or managing servers
	Lambda @Edge	Functions on Azure IoT Edge	–	Runs functions at the edge (directly on IoT devices) even with intermittent cloud connectivity
Batch computing	AWS Batch	Azure Batch	–	Runs large-scale parallel and high-performance computing applications efficiently in the cloud
Scalability	AWS Auto Scaling	Virtual Machine Scale Sets Azure Auto Scaling	Instance Groups	Service allowing customers to automatically change the number of instances providing a particular compute workload; configure defined metric and thresholds that determine if the platform adds or removes instances

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Management and Monitoring				
Cloud advisor	Trusted Advisor	Azure Advisor	Cloud Platform Security	Provides analysis of cloud resource configuration and security so subscribers can ensure they're making use of best practices and optimum configurations
Deployment orchestration (DevOps)	CloudFormation	• Azure Resource Manager VM extensions • Azure Automation	Cloud Deployment Manager	Provides a way for users to automate manual, long- running, error-prone and frequently repeated IT tasks
Management and monitoring (DevOps)	CloudWatch	Azure Portal Azure Monitor	• Stackdriver Monitoring Cloud Shell Debugger Trace Error Reporting	A unified console that simplifies building, deploying and managing cloud resources
	AWS Usage and Billing Report	Azure Billing API	Cloud Billing API	Services to help generate, monitor, forecast and share billing data for resource usage by time, organization or product resources
	AWS Management Console	Azure Portal	Google Cloud Console	A unified management console that simplifies building, deploying and operating cloud resources

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Management and Monitoring (Continued)				
Deployment orchestration (DevOps)	AWS X-Ray	Azure Application Insights + Azure Monitor	Stackdriver Monitoring Debugger Trace Error Reporting	An application performance management service for web developers on multiple platforms, this lets them monitor live web applications, detect performance anomalies and diagnose issues
Administration	AWS Application Discovery Service	Azure Log Analytics	Cloud Console	Provides deeper insights into applications and cloud workloads by collecting, correlating and visualizing all machine data, such as event logs, network logs and
	Amazon EC2 Systems Manager	Operations Management Suite	Cloud Console	Enables continuous IT services and compliance through process automation and configuration management; helps automate complex and repetitive IT tasks

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Security, Identity and Access				
Authentication and authorization	Identity and Access Management (IAM)	Azure Active Directory / Premium	Cloud IAM, Cloud Identity- Aware Proxy	Control access to services and resources while offering data security and protection; create and manage users and groups, and set user permissions to allow and deny access to resources
	AWS Organizations	Azure Subscription and Service Management + Azure RBAC	Cloud IAM	Security policy and role management for working with multiple accounts
	Multi-Factor Authentication	Multi-Factor Authentication	2-Step Verification	Service designed to safeguard access to data and applications by requiring multiple forms of identity validation prior to authentication users; provides a range of verification options.
Encryption	Server-side encryption with Amazon S3 Key Management Service	Azure Storage Service Encryption	–	Provides encryption for data at rest
	Key Management Service CloudHSM	Key Vault	Cloud Key Management Service	Provides security and works with other services by providing a way to manage, create and control encryption keys stored in hardware security modules (HSMs)

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Security, Identity and Access (Continued)				
Firewall	Web Application Firewall	Application Gateway Web Application Firewall	–	A firewall that protects web applications from common web exploits; users can define customizable web security rules
	Security groups + network access control lists	Network Security Groups	Firewall	Provide basic firewall protection and ingress and egress control to virtual networks and/or specific cloud hosts
Security	Inspector	Security Center	Cloud Security Command Center	An automated security assessment service that improves the security and compliance of applications, this automatically assesses applications, hosts and networks for vulnerabilities or deviations from best practices
	Certificate Manager	App Service Certificates	–	Service that allows customers to create, manage and consume certificates seamlessly in the cloud
	AWS Shield	Azure DDoS Protection Service	Cloud Armor	Provides cloud services with protection from distributed denial-of-services (DDoS) attacks

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Security, Identity and Access (Continued)				
Directory services	AWS Directory Service + Windows Server Active Directory on AWS	Azure Active Directory Domain Services + Windows Server Active Directory on Azure IaaS	–	Identity and access management cloud solution that provides a robust set of capabilities to manage users and groups
	Cognito	Azure Active Directory B2C	–	A highly available, global, identity management service for consumer- facing applications that scales to hundreds of millions of identities
Compliance	AWS Artifact	Service Trust Platform	–	Provides access to audit reports, compliance guides and trust documents from across cloud services

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Networking				
Cloud Virtual Networking	Virtual Private Cloud (VPC)	Virtual Network	Virtual Private Cloud	Provides an isolated, private environment in the cloud; users have control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways
Cross-premises connectivity	AWS VPN Gateway	Azure VPN Gateway	Cloud VPN	Provides secure VPN connections between on- premises and cloud- based workloads over the internet
Domain name system management	Route 53	Azure DNS Traffic Manager	Google Domains Cloud DNS	Service to manage your DNS records and hosts' domain names, plus routes users to internet applications, connects user requests to data centers, manages traffic to apps, and improves app availability with automatic failover
Content delivery network	CloudFront	Azure Content Delivery Network	Cloud Content Delivery Network	Global content delivery network that delivers audio, video, applications, images and other files

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Networking (Continued)				
Dedicated network	Direct Connect	ExpressRoute	Cloud Interconnect	Establishes a dedicated, private network connection from a location to the cloud provider (not over the internet)
Load balancing	• Classic Load Balancer • Network Load Balancer • Application Load Balancer	Load Balancer Application Gateway	Cloud Load Balancing	Automatically distributes incoming application traffic to add scale, handle failover and route to a collection of resources

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Storage				
Object storage	Simple Storage Services (S3)	Azure Storage – Block Blob	Cloud Storage	Object storage service for use cases including cloud applications, content distribution, backup, archiving, disaster recovery and big data analytics; typically used for content logs and files
Virtual server disk infrastructure	Elastic Block Store (EBS)	Azure Storage – Page Blob	Persistent Disk	SSD storage optimized for I/O intensive read/write operations; typically used for VHDs or other random- write type data
Shared file storage	Elastic File System	Azure Files	Cloud Filestore	Provides a simple interface to create and configure file systems and share common files
Backup / archival storage	Glacier / S3 Infrequent Access Data Archive	Azure Backup Storage (Cool) / Storage (Archive)	Cloud Storage Nearline / Cloud Storage Coldline	Backup and archival solution allowing files and folders to be backed up and recovered from the cloud and provides off- site protection against data loss; consists of two components: the software service that orchestrates backup/ retrieval and the underlying backup storage infrastructure

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Storage (Continued)				
Bulk data transfer	AWS Import/ Export Disk	Import/Export	Data Transfer Service	Data transport solution that uses secure disks and appliances to transfer large amounts of data; also offers data protection during transit
	AWS Import/ Export Snowball AWS Snowball Edge AWS Snowmobile	Azure Data Box	Transfer Appliance	Petabyte- to exabyte-scale data transport solution that uses secure data storage devices to transfer large amounts of data into and out of the cloud, at lower cost than internet-based transfers

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Marketplace				
Marketplace	AWS Marketplace	Azure Marketplace	GCP Marketplace	Easy-to-deploy and automatically configured third-party applications, including single virtual machine or multiple virtual machine solutions
Developer Resources				
Messaging	Simple Queue Service (SQS)	Azure Queue Storage	Cloud Pub/Sub	Provides a managed message-queuing service for communicating between decoupled application components
Workflow	Simple Workflow Service (SWF)	Logic Apps	–	Serverless technology for connecting apps, data and devices anywhere (on-premises or in the cloud) for large ecosystems of SaaS and cloud-based connectors
API management	API Gateway	API Management	Cloud Endpoints	A turnkey solution for publishing APIs to external and internal consumers
	Elastic Beanstalk	Web Apps Cloud Services API Apps	App Engine	Managed hosting platforms providing easy- to-use services for deploying and scaling web applications and services
	CodeDeploy CodeCommit CodePipeline	Visual Studio Team Services	–	Developer tools for scripting application

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Developer Resources (Continued)				
App customer payment service	Amazon Flexible Payment Service, Amazon Dev Pay	–	–	Cloud service that provides developers with a payment service for their cloud-based applications
DevOps	AWS CodeBuild	Visual Studio Team Services	Cloud Build	Fully managed build service that supports continuous integration and deployment
Backend process logic	AWS Step Functions	Logic Apps	–	Cloud technology to build distributed applications using out-of-the-box connectors to reduce integration challenges; connects apps, data and devices on-premises or in the cloud
Programmatic access	Command Line Interface	Azure Command Line Interface (CLI) Azure PowerShell	Cloud SDK	Built on top of the native REST API across all cloud services, various programming language- specific wrappers provide easier ways to create solutions
Predefined templates	AWS Quick Start	Azure Quickstart templates	–	Community-led templates for creating and deploying virtual machine–based solutions

Comparison of AWS, Azure and GCP Cloud Services				
Area	**AWS Service**	**Azure Service**	**GCP**	**Description**
Internet of Things (IoT)				
Internet of Things	AWS IoT Other Services (Kinesis, Machine Learning, EMR, Data Pipeline, SNS, QuickSight)	Azure IoT Suite (IoT Hub, Machine Learning, Stream Analytics, Notification Hubs, PowerBI)	Cloud Dataflow, Cloud IoT Core	Provides a preconfigured solution for monitoring, maintaining and deploying common IoT scenarios
Edge compute for IoT	AWS Greengrass	Azure IoT Edge	Cloud IoT Edge	Managed service that deploys cloud intelligence directly on IoT devices to run in on-prem scenarios

BGD e-GOV CIRT Service Offer

Cyber Sensors Unit

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.

Benefits

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.

Services

1. Manual attack traffic patterns analysis and incident detection (threat hunting)
2. Suspicious Traffic analysis
3. Anomaly detection
4. indexing and graphical review platform to index all events for deeper analysis

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)

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.

- 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.

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

Incident Handling Unit

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.

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.

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

IT AUDIT Unit

Auditor(s) To-Do List for the customers as follows,

1. Performing Audit
2. Prepare Audit Scope
3. Preparing Audit Framework for specific customer
4. Consulting with the documentation gap filling
5. Preparing Audit Engagement Letter and/or Audit
6. charter
7. Preparing Audit Terms of Reference (TOR) for the
8. resources
9. Future Predictive or future roadmap to the customer
10. for complying with the next Audit period
11. Conducting Training
12. Not limited to above

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

Threat Intelligence Service

BGD e-GOV 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.

Service detail	Package name	Fee
▪ 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.

Service(s) Payment Terms

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.