

# Information Security for an Information Society in Bangladesh

A dissertation submitted to the  
Department of Management Information Systems (MIS)  
in partial fulfillment of the requirements for the Degree of  
**Doctor of Business Administration (DBA)**



Submitted by:  
**Md. Kamruzzaman**  
Department of Management Information Systems

Submitted to:  
**Professor Dr. Md. Hasibur Rashid**

Department of Management Information Systems (MIS)  
Faculty of Business Studies (FBS)  
University of Dhaka.  
Date of Submission: **April 5, 2023.**


# **'INFORMATION SECURITY FOR AN INFORMATION SOCIETY IN BANGLADESH'**

## DECLARATION

I hereby declare that the dissertation paper entitled “Information Security for an Information Society in Bangladesh” Submitted for the degree of Doctor of Business Administration is my original work and this work has not been formed the basis for the award of any other degree, association, fellowship or any other similar title.

Place: Dhaka

Date: 5 April 2023



(Signature of the Researcher)

Name: Md. Kamruzzaman

**CERTIFICATE BY SUPERVISOR FOR RESEARCH PAPER / DISSERTATION**

**CERTIFICATE**

This is to certify that the doctoral study entitled “Information Security for an Information Society in Bangladesh” is a bonafide research work carried out by Mr. Md. Kamruzzaman, Joint Secretary of the Government of the People’s Republic of Bangladesh, a student of Department of Management Information Systems (MIS), Faculty of Business Studies (FBS) of the University of Dhaka, under my direct supervision.

This research work has been found to be complete and satisfactory in all respects and that all revisions required by the review committee have been made.

I therefore recommend it to the Dean of FBS for further necessary action.

Place: Dhaka  
Date: April 5, 2023



(Signature of the Supervisor)

Professor Dr. Md. Hasibur Rashid  
Department of Management Information Systems  
Faculty of Business Studies  
University of Dhaka

&

Vice Chancellor  
Begum Rokeya University,  
Rangpur, Bangladesh

## Acknowledgement

First and foremost, I would like to say الحمد لله (Alhamdulillah) for reaching to the end of this research work.

A good number of people have contributed directly or indirectly to the development of this dissertation. In terms of getting insights into the theme, argument on different topic, constructive criticism and guidance on my draft work and overall encouragement to go ahead, I would like to thank my thesis advisor Professor Dr. Md. Hasibur Rashid. His enthusiastic comments and ingenious vision really enhanced the content of the paper.

I am truly indebted to the respondents of the various organizations of Bangladesh Government. Even in the pandemic situation, they showed utmost responsibilities to get my interview questions well answered. I would like to extend my special thanks to the PD of BGD e-GOV CIRT for providing technical clarification of numerous Information Security issues as the Key Informant.

I am also grateful for having such a distinguished appreciation and supportive feelings from Professor Dr. Dip Nandi, Director, Computer Science and Engineering, Faculty of Science and Technology of American International University-Bangladesh (AIUB) at the time of arranging the contents of this dissertation. Thank you so much for providing the needed advice and guidance in meeting my prospectus, proposal and final documentation requirements.

I acknowledge with thanks and gratitude for the support, help and cooperation I received from the esteemed fellow Course Members, Professors of the MIS department and concerned office staff of Faculty of Business Administration (FBA). I also express my heartfelt thanks and sincere gratefulness to them.

I sincerely express my indebtedness to my beloved parents Alhaj Md. Abdur Rashid and Begum Shamsunnahar Rashid for their everlasting patience, unconditional support, and inspiration towards my aspirations. Therefor, this doctoral study is dedicated to my pragmatic parentage.

Last, but not least, I extend my deepest sensation and affection to my loveliest daughters Suzana Fatin Zaman and Suhana Fatin Zaman who have been a constant source of encouragement, pleasure, and happiness in my life.



Md. Kamruzzaman  
April 5, 2023  
Dhaka, Bangladesh.

# **Information Security for an Information Society in Bangladesh**

## **Abstract**

Nowadays, public institutions are heavily dependent on modern technology for their office management in Bangladesh. The advancement of modern technology in today's world has a great influence in daily life. Along with the positiveness of the advancement, somewhere the scope for the negativities tends to increase. As dependency on modern technology and information technology increases, the rate of negative impacts tends to increase as well. Specifically on the performance of Information Systems and therefore they become more exposed to the continuous evolving security risks and vulnerabilities inherent to the momentous growth of digitalization. A semi-structured questionnaire and an experienced key informant's interview have thoroughly been analyzed during the research. This research focuses on the impacts and necessities of Information Security for an Information Society considering the government organizations only because the government organizations are one holding access to the national database. The findings of this qualitative research indicate what sort of Information threats are being encountered by Bangladeshi public enterprises, how are they managing the major Information threats and what they really need to do if they want to get well ahead of recent cyber criminals' activities. The study as well includes some of the recent national and international cyber security attack incidents, their impacts and the organization's attempts to reduce the loss of the attack. The loss and damage already caused by some attacks during the previous decade, made serious impact on organization's business continuity, reputation, and loss of asset. Sometimes, even the organizations fail to recognize that their security system has already been compromised. Recently, UK-based National Cyber Security Index Report 2021 unveils the fact that Bangladesh has made commendable progress in improving the foundation of its Information security system. Bangladesh Government has formed an e-Government Computer Incident Response Team (BGD e-GOV CIRT), that has been serving as the National CIRT of Bangladesh (N-CERT). They are engaged in receiving, reviewing, and responding to computer security related incidents and activities within Bangladesh. The organization

holds collaboration with international organizations as partners to ensure security in cyberspace. In addition, the goal of the organization is being quick reactive towards security threat and actively reporting as well. However, a good number of literatures and respondents of this study delineate the fact that existing level of security is moderate to good where there is still a lot more to do. Adequate security procedures to manage information security, appropriate office equipment's along with proper employee trainings are obviously required and organizations need to carefully evaluate their security policies to enhance security infrastructures. The enhancements will act as a shield to protect organizations from future threats. Superior Information Security management can help the nation to expand, and the Government of Bangladesh (GoB) supports such advancements along with the improvements and leaves no stone unturned in supporting the organizations. Currently, corporations' approaches to information security go beyond the fundamentals. They have gradually been adapting their security strategies based on Information Security Policy guidelines 2014 and ISO/IEC 27003 standard ISMS implementation guidance. Authorities must alter the way they think of just responding to threats instead look around necessary measures or possibilities of future threats to prevent or overcome the threats. In addition, the authorities need to analyze, study the security attack incident reports, patterns in order to detect certain pattern or data that may give future lead. Apprehending of Information attack is the most suitable way to be ahead of Cyber espionage. Upon such practices, public institutions will become more difficult to deal with as opposed to being an easy target. As a result, public and organization's satisfaction remains retained.

## TABLE OF CONTENTS

Serial	Contents	Pages
	Preliminary pages	<b>i-xxv</b>
	<i>Cover Page</i>	i
	<i>Research Title</i>	ii
	<i>Declaration</i>	iii
	<i>Certificate by the Supervisor</i>	iv
	<i>Acknowledgement</i>	v
	<i>Abstract</i>	vi
	<i>Table of Contents</i>	viii
	<i>List of Tables</i>	xi
	<i>List of Figures</i>	xii
	<i>List of Annexes</i>	xiii
	<i>List of Abbreviations</i>	xiv
	<i>Glossary of Terms</i>	xvii
<b>1.</b>	<b>Chapter I: Introduction</b>	<b>1-18</b>
1.1	Background of the Study	1
1.2	Research Problem	6
1.3	Significance of the Research Problem	10
1.4	Scope of the Study	13
1.5	Objectives of the Study	14
1.6	Research Questions	15
1.7	Limitations of the Study	15
1.8	Justification of the Research	16
1.9	Structure of the Thesis	17
<b>2.</b>	<b>Chapter II: Literature Review</b>	<b>19-58</b>
2.1	Overview	19
2.2	Information Security Management Systems (ISMS)	19
2.2.1	ISMS Concepts	21
2.2.2	ISMS in the Public Sector	22
2.2.3	Role of Various Standards	25
2.2.4	Socio-Technical Perspectives	37
2.3	Organizational Culture	39
2.3.1	Organizational Culture (Bangladesh e-government initiative)	40
2.3.2	Relationship between ISMS and Organizational Culture	41
2.4	Areas of Exploration	42
2.5	Framework for Improving Critical Public Infrastructure Cybersecurity	42
2.6	Policy Implementation	54
<b>3.</b>	<b>Chapter III: Theoretical Framework</b>	<b>59-63</b>
3.1	Overview	59
3.2	Relevant Theories	59
3.2.1	Grounded theory	59
3.2.2	Socio-technical system theory	60
3.2.3	Socio-psychological theory	60



<b>Serial</b>	<b>Contents</b>		<b>Pages</b>
	3.2.4	General deterrence theory	61
	3.2.5	Institutional theory	61
	3.3	Conceptual Framework for this Research	62
	3.4	Relevant Values of the Institutional Culture	63
	3.5	Implication of Theories in Information Security Research	63
<b>4. Chapter IV: Research Methodology</b>			
	4.1	Overview	64
	4.2	Justification of the Methodology	64
	4.3	Sampling Procedure	65
	4.4	Source of Data Collection	66
	4.4.1	Government Organizations as Data Source	66
	4.4.2	Primary data	69
	4.4.2.1	Interview	69
	4.4.2.2	Personal Observation	69
	4.4.2.3	Key Informant Interview	69
	4.4.3	Secondary data	70
	4.5	Data Interpretation	70
	4.6	Validity and Reliability	71
	4.7	Problems, Challenges and Limitations	71
<b>5. Chapter V: ICT Perspective for Information Society</b>			
	5.1	Overview of the progress	72
	5.2	Achieving SDGs	86
	5.3	Areas for further improvement for an information Society	94
	5.4	Strategic direction adopted for Information Society	95
	5.5	Creating an Information based economy	96
	5.5.1	Digital Opportunities and Innovation	97-104
	5.5.2	Leveraging 4IR to achieve knowledge-based economy	
	5.5.3	Moving from factor-based stage to Information based economy	
	5.5.4	Building Transport and Communications Infrastructure for sustained growth	
<b>6. Chapter VI: Analysis and Findings</b>			
	6.1	Overview	105
	6.2	Identity of studied organization	106
	6.2.1	Bangladesh Bank	106
	6.2.2	Election Commission	111
	6.2.3	Bangladesh Police	113
	6.2.4	Land Records and Survey Department	116
	6.3	Interview Analysis	119
	6.3.1	Present Situation of ISMS and Governance Structure	119
	6.3.1.1	Organizational IT Setup	121
	6.3.1.2	Information Security Incidents, associated threats etc.	142
	6.3.1.3	Preventive Technologies	147

<b>Serial</b>	<b>Contents</b>		<b>Pages</b>
	6.3.1.4	Safeguarding and Reactive Measures to the Incidents	150
	6.4	Personal Observations	152
	6.5	Key Informant Interview	154
	6.5.1	Experience of on-going Risks, Threats and Vulnerabilities	154
	6.5.2	The results of existing protection mechanisms	156
	6.5.3	Information Security consciousness inside the institutions	156
	6.5.4	Auditing and testing of Information Security policies	156
	6.5.5	Organization's Thinking on Better Security Level	157
	6.5.6	Business Continuity Plan for Disaster events	157
	6.6	Major Findings	158
<b>7.</b>	<b>Chapter VI: Discussion and Ways Forward</b>		<b>159-173</b>
	7.1	Overview	159
	7.2	Emerging Critical Threats	159
	7.2.1	General Symptoms related to Cyber Attack	159
	7.2.2	What if the systems get infected	159
	7.3	Impact of Covid-19 on Organizations Information Security Budget	160
	7.4	Best Practices to handle Information Incidents	162
	7.4.1	Common Users	163
	7.4.2	Home Users	164
	7.4.3	Use of social media	165
	7.4.4	Use of Smart Phones	167
	7.4.5	Dealing with Employee Risks	168
	7.4.6	Protecting Employees from Covid-19 situation	168
	7.5	Develop Information Security Culture in Public Organizations	168
	7.5.1	Role of Organization's Governance	170
	7.5.2	Launching Framework for Security Awareness	170
	7.5.3	Skillful Information Security Professionals	171
	7.5.4	Organizational Information Security Policy	172
<b>8.</b>	<b>Chapter VIII: Recommendations and Conclusion</b>		<b>174-192</b>
	8.1	Overview	174
	8.2	Recommendations	174
	8.3	Implications	189
	8.4	Indication for Future Research	189
	8.4.1	Future Scope	190
	8.5	Objective fulfillment	191
	8.6	Conclusion	191
<b>References</b>			<b>I-XV</b>
<b>Annexures</b>			
1.	Interview Questionnaire		A
2.	NCSI Report		B-C

## LIST OF TABLES

<b>Table no</b>	<b>Title</b>	<b>Page</b>
Table 6.1	Top Information Threats in Bangladesh 2020	155

## **LIST OF FIGURES**

<b>Figure no</b>	<b>Title</b>	<b>Page</b>
Figure 2.1	Corporate ISG literature review organization	40
Figure 2.2	NIST framework to protect critical cybersecurity infrastructure	48
Figure 2.3	SOC Architecture	50
Figure 3.1	Steps in Grounded Theory	60
Figure 3.2	The Conceptual framework of the study	62
Figure 5.1	Four pillars of Digital Bangladesh	77
Figure 5.2	Realization position of SDGs by the ICTD	88
Figure 6.1	National Cyber Security Index version 23	154
Figure 6.2	Information Security Compliance Structure	157

**LIST OF ANNEXES**

<b>Annex</b>	<b>Title</b>	<b>Page</b>
Annex A	Interview Questionnaire	A
Annex B	NCSI report	B-C

## LIST OF ABBREVIATION

Abbreviation	Full form
<b>A</b>	
AFWC	Armed Forces War Course
APCERT	Asia Pacific Computer Emergency Response Team
API	Application Programming Interface
APT	Advanced Persistent Threat
<b>B</b>	
BASIS	Bangladesh Association of Software and Information Services
BB	Bangladesh Bank
BBC	British Broadcasting Corporation
BCC	Bangladesh Computer Council
BCS	Bangladesh Computer Samity
BGD e-GOV CIRT	Bangladesh Government's e-Government Computer Incident Response Team
BMS	Building Management System
BPO	Business Processing Outsourcing
BTRC	Bangladesh Telecommunication Regulatory Commission
<b>C</b>	
CCA	Controller of Certifying Authorities
CCTV	Close Circuit Television
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIRT	Computer Incidence Response Team
CISO	Chief Information Security Officer
CIA	Confidentiality, Integrity and Availability (of Data/Information)
CII	Critical Information Infrastructure
COBIT	Control Objectives for Information and Related Technology
CPA	Cyber Physical Attack
CTDR	Cyber Threat detection and Response
<b>D</b>	
DCS	Digital Control System
DDoS	Distributed Denial of Services
DLRS	Directorate of Land Records and Survey
DoICT	Department of Information and Communication Technology
DPI	Deep Packet Inspection
DPO	Data protection officer
DSA	Digital Security Agency
DoS	Denial of Services
<b>E</b>	
EC	Election Commission
ENISA	European Union Agency for Network and Information Security
EOP	Emergency Operation Procedure
EU	European Commission
<b>F</b>	
FBI	Federal Bureau of Investigation

<b>Abbreviation</b>	<b>Full form</b>
<b>G</b>	
GCI	Global Cyber-Security Index
GDP	Gross Domestic Product
GEIT	Graphic Era Institute of Technology
GoB	Government of Bangladesh
GPS	Global Positioning System
<b>H</b>	
HCI	Human Computer Interaction
HTTPS	Hypertext Transfer Protocol Secure
<b>I</b>	
ICTD	Information and Communication Technology Division
IDG	International Data Group
IDS	Intrusion Detection System
IEC	International Electro-technical Communication
InfoSec.	Information Security
IoT	Internet of Things
IPS	Intrusion Prevention System
IS	Information System
ISG	Information Security Governance
ISMS	Information Security Management System
ISO	International Organization for Standards
ISPAB	Internet Service Providers Association of Bangladesh
ISPG	Information Security Policy Guidelines
IT	Information Technology
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
IP	Internet Protocol
<b>J</b>	
<b>K</b>	
<b>L</b>	
LAN	Local Area Network
LFI	Local File Inclusion
<b>M</b>	
MoF	Ministry of Finance
MoHA	Ministry of Home Affairs
MoPTIT	Ministry of Posts, Telecommunications and Information Technology
MoU	Memorandum of Understandings
MFS	Mobile Financial Service
<b>N</b>	
NCSI	National Cyber Security Index
NDC	National Defense Course
NDSC	National Digital Security Council
NIST	National Institute of Standards and Technology
NRI	Network Readiness Index

<b>Abbreviation</b>	<b>Full form</b>
<b>O</b>	
OECD	Organization for Economic Cooperation and Development
OWASP	Open Web Application Security Project
<b>P</b>	
PC	Personal Computer
PD	Project Director
PDCA	Plan-Do-Check-Act Cycle
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PMIS	Personnel Management Information Systems
PSC	Passed Staff College
<b>R</b>	
RoR	Record of Rights
R&D	Research and Development
<b>S</b>	
SAARC	South Asian Association for Regional Cooperation
SB	Special Branch (of Bangladesh Police)
SDG	Sustainable Development Goal
SME	Small and medium-sized companies (SMEs)
SOC	Security Operation Center
SOP	Standard Operation Procedures
STEM	Science, Technology, Engineering and Management
SWIFT	Society for Worldwide Interbank Financial Telecommunication
Sysadmin	System Administrator
SSL	Secure Sockets Layer
<b>T</b>	
ToT	Training of Trainers
TLS	Transport Layer Security
<b>U</b>	
UNB	United News Bangladesh
USD	United States Dollar (currency)
URL	Uniform Resource Locator
<b>V</b>	
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
<b>W</b>	
WAN	Wide Area Network
<b>X</b>	
XSS	Cross-Site Scripting
<b>Y</b>	
<b>Z</b>	



## GLOSSARY OF TERMS

<b>Glossary of Terms</b>	<b>Definitions</b>
Agency	Agency incorporates all Ministries/Divisions, Departments and Sub-ordinate offices of GoB under section 5 of DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018.
Anti-Virus	A program that tracks a computer or network for the detection of all significant malicious programs and the prevention or containment of malware incidents. NIST-2011.
Asset	Asset is an item of property owned by a person or company, regarded as having value and available to meet debts, commitments, or legacies.
Attack	Act with a view to destroy, reveal, change, damage, theft or obtain unwarranted access to or illegal use of an asset
Authentication	Provision of guarantee that an argued attribute of a unit is accurate.
Authenticity	Quality of an entity is what is claims to be
Availability	The communication system is available to legitimate consumers at any predetermined or defined time, and it is ensuring access upon requirement by an authorized entity.
Awareness (Information Security)	NIST-2011 defines activities that seek to focus an individual's attention on a (information security) issue or set of issues.
Block Chain	A block chain is a series of data blocks linked together by cryptographic hash functions that prevent the data contained in the blocks from being tampered with.
Botnets	Botnet is a network of malware infected computers which is controlled by a single hacker. In most cases, botnets are used to accomplish DDoS attacks.
Breach	A security breach that results in the unintentional or unlawful destruction, loss, alteration, unauthorized disclosure, or access of protected data transferred, stored, or otherwise processedS.
Business Continuity	Plan of action to make sure for keeping up business activities
CERT	The "National Computer Emergency Response Team (CERT)" or the Computer Emergency Response Team constituted under section 9 of the DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018, is referred to as the Computer Emergency Response Team (CERT).

<b>Glossary of Terms</b>	<b>Definitions</b>
Certification	It is anything that any regulatory authorities or environment analysis come up with after evaluating an organization's IS architecture and ISMS.
Classified Information	Those types of information, recognized as confidential in accordance with the concern agency's Security Regulations. The importance, legal requirements, sensitivity, and criticality of information to the country or agency can all be classified.
Confidentiality	Data/Information is not made accessible or disclosed to unwanted persons, entities, systems or processes.
Control	It refers to the policies, methods, principles, practices, or institutional arrangements that govern risk in an institution. These policies, procedures, guidelines, practices, or institutional arrangements can be administrative, technical, management-related, or legal in character.
Control objective	Describe what will be accomplished as a result of the use of controls.
Corrective action	Taking measures to remove the origin of an identified violation or other unacceptable situation.
CII	"Critical Information Infrastructure (CII)" refers to any external or virtual information infrastructure declared by the government that controls, processes, circulates, or preserves any information-data or electronic information and, if damaged or critically affected, may have a negative impact on other information-data or electronic information. <ul style="list-style-type: none"> <li>(i) public safety, financial security, or public health;</li> <li>(ii) national security, national integrity, or sovereignty and</li> <li>(iii) national security, national integrity, or sovereignty</li> </ul> According to section 2(g) of DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018.
CIRT	This organization, sometimes known as a 'Computer Incident Response Team,' is in charge of responding to security breaches, viruses, and other potentially catastrophic situations in businesses with substantial security threats.
Critical Infrastructure	It is systems and resources, either physical or digital, that are

Glossary of Terms	Definitions
	so vital to a state that their incapacity or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination of those issues.
Crypto jacking	It is a kind of cyber incident where cyber criminals' hack into an organization's PCs, laptops and other portable devices to install malicious software.
Cyber Espionage	The use of computer networks to gain unauthorized access to secret information held by the government or other similar organizations.
Cyberspace	A worldwide domain inside the digital world consisting of an interconnected network of information systems, infrastructures, and computer systems, embedded processors, and controllers, including the internet, telecommunications networks, and computer systems. Cybersecurity, cyber-power, and cyber warfare are all part of the cyberspace.
Cyber Physical Attack	Cyber-attacks have the potential to damage physical assets-utilities and industrial infrastructure.
Cyber Power	It is the capability of an individual, an organization, or a nation-state using cyberspace to explore advantages effectively and efficiently. Cyber power is a measure or the degree of ability to control, manipulate and influence cyberspace.
Cyber Security	Cyber security is a collection of technologies, processes, and practices aimed at preventing attacks, damage, and illegal access to networks, devices, programs, and data.
Data Breach	Data breach is a cyber incident where information being theft or stolen from a network-based system without the permission from the owner of the information. U.S. Government Accountability Office, 2007.
Deep Packet Inspection	DPI is a scientific method to scan the element of data packet when they go through a control point within a network system.
(D) Denial of Services (DoS)	An attempt to render a system or network resource inaccessible to its intended users (distributed) denial-of-service.

Glossary of Terms	Definitions
Digital	"Digital" refers to a working method based on double digit (0 and 1/binary) or digit, and includes electrical, digital, magnetic, optional, biometric, electrochemical, electromechanical, wireless, or electro-magnetic technology for the purposes of this Act. According to section 2(i) of DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018.
Digital device	"Digital device" refers to any electronic, digital, magnetic, optical, or information processing device or system that uses electronic, digital, magnetic, or optical impulse to perform logical, mathematical, or memory functions and is connected to any digital or computer device system or computer network, as well as all types of input, output, processing, accumulation, digital device software, or communication facilities; According to section 2(j) of DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018.
Digital Security	"Digital security" refers to the protection of any digital device or system.; According to section 2(k) of DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018.
Disclosure	An infraction wherein data was actively revealed (rather than just exposed) to an unidentified user.
Disinformation	Disinformation is wrong or erroneous information intentionally spread with malicious intent to misleading, confusing or manipulating an audience.
Eavesdropping	This is also an illegal access to information by seizing packets while travelling/transmission of information.
Encryption	The technique of encoding messages or information in such a way that it can only be read by authorized persons.
Exploit	An action, approach or codes that manipulate a vulnerability to make system access to the attacker.
Firewall	A hardware/software capability that restricts network and/or system access in accordance with a security policy. National Institute of Standards and Technology, 2011.
Guidelines	A declaration that explains how and what to do, to attain the objectives exhibited in policies for any information system,

Glossary of Terms	Definitions
	service or infrastructure, or the physical locations accommodate them.
Hacker	Unapproved individual who tries to or succeeds in gaining access to a computer system. National Institute of Standards and Technology, 2011.
Identity Theft	Identity theft occurs when cybercriminals obtain a victim's personally identifiable information (PII) (such as their name, social security number, or credit card details without their permission in attempt to commit fraudulent acts.
Incident	A privacy event that jeopardizes an information asset's Confidentiality, Integrity, or Availability (CIA).
Information Leakage	When a system designed to keep an eavesdropper out leaks some information to unauthorized persons, it is called information leakage.
Information System (IS)	Computer systems, servers, workstations, terminals, storage media, communication devices, network resources, and the Internet are all examples of systems that operate data electronically through the application of Information Technology.
Information	Information is a collection of data in an intelligible format that can be shared. Information is a valuable asset that affects a company's operations and must be properly protected.
Information Assets	Data assets are valuable goods that hold data (Davis, 2012).
Information Security	In addition to authenticity, accountability, non-repudiation, and reliability, CIA data/information security can be complicated. (Martins & Veiga, 2015).
Information Security Governance (ISG)	"A subset of enterprise governance that offers strategic direction, ensures that objectives are met, manages risks correctly, uses organizational resources responsibly, and monitors the success or failure of the enterprise security [program]," according to ISG (ITGI, 2008, p. 18).
Information Security Policy	A set of management instructions that spell out how to properly use and manage computer and network resources in order to safeguard these assets, as well as the data stored or processed by Information Systems, from unauthorized

<b>Glossary of Terms</b>	<b>Definitions</b>
	disclosure, modification, or destruction.
Information Security Event	It is a previously unknown scenario or an identified incidence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards.
Information Security Incident	A single or a sequence of unwanted or unexpected events that have a high likelihood of jeopardizing business operations and endangering information security constitute an information security incident.
Infrastructure	Network components, such as switches, routers, firewalls, and servers.
IP Address	A a unique label given to each machine or printer connected to a computer network utilizing the Internet Protocol (IP).
Insider Threat	Workers, former employees, contractors, or business associates who have inside information about the organization's security policies, data, and computer systems pose a harmful threat to the firm.
Integrity	When permitted individuals could make modifications to the data stored or processed by Information Systems in any situation.
Internet of Things (IoT)	The connecting actual items or "things" that have electronics, software, sensors, and connections embedded into them so they can communicate data with the maker, operator, and/or other connected devices to provide better value and service. The embedded computing system in each object allows for unique identification and allows for communication with other objects on the Internet(s).
Malware	Software or firmware designed to carry out an unlawful process that compromises an Information System's Confidentiality, Integrity, or Availability. Infecting a host with a virus, worm, Trojan horse, or other code-based entity. Malicious code also includes spyware and some types of adware.
Mobile devices	Smartphones, tablets, netbooks, laptops.
Misinformation	Whether or not it's meant to mislead or deceive individuals, misleading information is referred to as misinformation.

Glossary of Terms	Definitions
Network	A collection of interconnected components is used to create an information system. Routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices are examples of such components. National Institute of Standards and Technology, 2011.
Password	A string of characters (letters, numbers, and other symbols) used to validate access authorization or authenticate an identity. 2011 National Institute of Standards and Technology
Performance Management	To guarantee that organizational objectives are met, performance measurement entails quantifying, monitoring, and reporting the performance of information security systems, processes, and related activities (ITGI, 2008).
Person	According to section 2(p) of the DIGITAL SECURITY ACT, 2018 Act No. XLVI of 2018, "person" means any person or institution, company, partnership business, firm, or other organization, or in the case of a digital device, its controller, as well as any entity created by law or any artificial legal entity;
Phishing	Using fraudulent computer-based methods to trick people into providing sensitive personal information. The deceitful practice of sending emails that look to emanate from reputable companies in order to get personal information such as passwords and credit card numbers from recipients.
Physical Manipulation	In essence, data manipulation is a deceptive cyber activity in which a malicious actor alters, tweaks, or modifies valuable digital documents and critical data rather than stealing it outright in order to harm the company and cause havoc.
PKI	PKI is a key and certificate management framework that includes hardware, software, network, policies, and processes.
Policy	The overall goal and regulation of an organization as explicitly expressed by the administrative wing.
Ransomware	A form of malware that limits access to systems it infects and demands a ransom payment to the infection's creator(s) in order to remove the restriction.
Resource Management	Manager-leaders' purpose for optimal investment in and proper administration of information security resources is

<b>Glossary of Terms</b>	<b>Definitions</b>
	referred to as resource management (Mohare & Lanjewar, 2012; Davis, 2008; Yaokumah, 2013).
Risk Analysis	Methodical application of data to identify genre, sources, and risk estimates.
Risk Assessment	The entire risk analysis and risk appraisal procedure.
Risk Evaluation	The process of comparing an estimated risk to a set of risk criteria to evaluate the significance of an impending issue.
Risk Management	Organized risk management operations that direct and control an organization. Rasheed, ChangFeng, and Yaqub (Rasheed, ChangFeng, & Yaqub, 2015).
Risk Treatment	Selection and implementation of risk-control or risk-minimization measures.
Social Engineering	Using deception to obtain information from computer/network users.
Spam	Electronic junk mail refers to the use of electronic communications networks to send unsolicited bulk messages to anyone.
Spoofing	A type of bluffing in which a trustworthy IP address is used to gain access to a computer system instead of the genuine IP address.
Strategic alignment	Ensure enterprise, IT, and information security plan linkage; define, manage, and validate the information security value proposition; and information security operational congruence with business and IT operations are all important aspects of strategic alignment (Davis, 2008).
Third Party	That individual or organization that is acknowledged as being independent of the ISMS participants.
Threat	An action that could cause source of an undesirable event that could impair a system or an organization's data assets.
Trojan	A software application that appears to perform a helpful job but secretly performs a hidden and potentially malicious function that circumvents security safeguards, sometimes by leveraging genuine authorizations of the system entity that invokes the program.
Value delivery	Throughout the delivery cycle, value delivery refers to



<b>Glossary of Terms</b>	<b>Definitions</b>
	implementing the information security value proposition and ensuring that information security delivers asserted benefits in line with chosen organizational strategies (Davis, 2008).
Vulnerability	Vulnerabilities are defects in system design, architecture, production or implementation with an agency's systems, assets or capabilities.
Web Application Attack	An effort by a malevolent actor to undermine the security of a web-based program is known as a web application attack.
Web based attack	Application-layer attacks are a form of cyber vandalism danger that occurs when thieves use coding flaws to obtain access to a server or database.
Worm	A networking-based program that is self-replicating, self-propagating, and self-contained.

# CHAPTER I: INTRODUCTION

## 1.1 Background of the Study

Information has always been regarded as priceless as wealth for an organization as in the current era, there is a great, urgent, and continuous need of information for various aspects. In today's world, Information and Communication Technology (ICT) has become a vital part of the learning process. Technology's advancement and progress are having a significant impact on higher education. It is subjected in the preparation of various learning concepts in order to improve the impact of teaching, learning, and research criteria. It emphasizes the various effects of information and communication technology on development and the generation of various approaches. This application of the given technology has altered business and governance operations (Viney Dhiman and Anupama Bharti, 2022). The online learning techniques provide an opportunity to use appropriate factors of consideration to educational research in order to develop a decent method of appropriate learning based on various analysis. It is the curriculum's method for creating a demand for educational practices. From the increasing usage of Information and Communication technology, the usage of information in several sector has an upward trend. This as a result leads to protecting information or data from being misused. Such as, Government Information has distinct aspect with respect to availability and usability in terms of making policies or taking decisions (Posthumus and Solms, 2004). Some information is public on the other hand some are restricted, confidential, secret, and top secret in nature. According to the level of secrecy, public information has some level of accessibility in government organization of Bangladesh. Therefore, it is very important for an institution to impose restrictions on its information, allow accessibility based on its value, maintain confidentiality in terms of sharing and handle data with safety to avoid unwanted usage.

Information security can be achieved through proper information system management. Every organization's functioning and administration rely on information systems. Managers who invest significant sums of money and other resources in information systems frequently have no idea which applications will assist the company. In today's world, Information security is a major concern and different

approaches, or concepts are proposed continuously to handle the problematic situation to overcome from it. Profiling side-channel attack, Intrusion Response Systems, The use of video steganography to convey various kinds of secret messages, Privacy preserving Cloud computing, Data confidentiality-preserving schemes, Malware detection techniques, Network anomaly detection and Adaptive reversible Data hiding are some of the recent works published on Information Security to tackle and prevent malicious activities against preserving Data security to uphold public and asset security of the nation. These techniques in general can be integrated with the existing systems to enhance privacy policies of the organizations. Information has discrete definitions but Information Security data deals with public data that maybe confidential, restricted, or personal thus, such data should be taken good care to avoid spreading or unwanted use by mischievous parties. Information security is about protecting the data from being leaked, mismatched, manipulated, and distorted. Both the receiver and sender must ensure that they are served with the correct data. In fact, some data can be manipulated to change result of any sort of evaluation that might be political or non-political. This concludes that data security management is important to maintain accuracy in judgement and evaluation of any process.

Information technology has been expanding to a great extend in the recent years. As there has been increasing urge or dependance of Information technology, this has given rise to some of the Information security or cyber security related incidents that have had great impact on the organization. Knowing what cyber security is and how to use it successfully is critical. If there is no security to secure it, systems, vital files, data, and other important virtual items are at risk. Every company, whether it is an IT firm or not, must be protected equally, data are not limited to IT firms only, every organization work on some sort of data that is important. The attackers, likewise, do not fall behind with the development of new cyber security technology. They are employing improved hacking tactics and focusing on the weak points of many businesses. As military, political, financial, medical, and corporate institutions collect, practice, and store vast amounts of data on PCs and other devices, cyber security is important to preserve those data (Mrs. Ashwini Sheth and Mr. Sachin Bhosale, 2021). All the above-mentioned data are very important and plays a crucial role towards a nation. If any of these data is leaked, the country's primary plan and execution will be altered.

As the number of people using the internet grows, so does the number of attacks. Bangladesh is ranked 2nd among all countries in terms of infection levels, as per the "*Kaspersky Security Bulletin 2015*." In Bangladesh, 69.55 percent of unique users are at the highest risk of contracting a local virus. According to Trend Micro's Global Spam Map, 80 percent of users are spam victims. The total number of targeted IP addresses in Bangladesh was 34552 in a two-hour test conducted by the Bangladesh Computer Council. IP addresses from well-known companies like as Banglalion, Grameen Phone, and Link3 can also be discovered in the list. Since a couple of years ago, Bangladesh has been confronted with countless number of malware occurrences in the form of infiltration in Banking system as well as non-banking organizations, such as web page disfigurement, dismantling of information, cyber espionage, misappropriation of information, Distributed Denial of Services (DDoS).

The level of the incurred threat was considered as high, and Bangladesh's e-Government Computer Incident Response Team (BGD e-Gov CIRT) reported that vulnerabilities were discovered in more than 200 servers of the Microsoft Exchange Servers (MES) of Bangladesh (Team, n.d.). According to the report the organizations included Bangladesh Bank (BB), Bangladesh Telecommunication Regulatory Commission, Dhaka Bank, Standard Bank, Trust Bank, Bank Asia, Evercare Management Group, Evercare Hospital Dhaka, Lanka-Bangla Finance, Bangla Trac Communications, and Agni Systems along with several reputable private and public organizations. The Government of Bangladesh at its earliest concern formed a group of BGD e-Gov CIRT under the Ministry of Posts, Telecommunications, and Information Technology to work on the incidents to reduce the impact of the occurrence and in future improve the country's overall cyber security infrastructure. In addition, be able to predict future possible attacks determining current attack patterns and future analysis. BGD e-GOV CIRT also conducts research and development projects based on the security threat issues and encountered vulnerabilities to improve future threat detection policy and minimize threat detecting time. It is thought that the shorter the threat detection time, the less damage is done. The Government of Bangladesh asked for the reports of the analysis of the incidents and stated necessary actions in order to improve the country's cyber security infrastructure. According to several observations, it has been stated that it took place due to the absence of Information Security (InfoSec) method, the way employees

behave towards the technology, their interests towards technical applications, fragile and unregulated security controls performed in organizations, uncontrolled device security and lack of knowledge of unskilled IT officials towards (Information Technology).

British Broadcasting Corporation (BBC) refers to a Federal Bureau of Investigation's (FBI) inquiry report which unveils the Bangladesh Bank (BB) heist in February 2016, hackers failed to steal the targeted USD 931 million. The hackers could manage to theft only USD 81 million through 05 (five) successful transactions out of 35 (thirty-five) efforts they made. The malware was not only patterned to amend the SWIFT transactions but also to hide their activities during the robbery. SWIFT is a messaging platform to transfer money internationally between banks. According to the statements, it has been said that the attacker was within the network of Bangladesh Bank. FBI investigations found that a spoofing e-mail was sent to some of the Bangladesh Bank (BB) officials and at least one of them stepped into the trap and clicked on the link to enable the entrance of the virus. The virus in the email entered the computer and got spread throughout the BB's entire network system. Once it entered the bank system, the hackers (North Korean Lazarus Group) managed to conduct several transactions to draw out money from the bank's account. It began working on the digital vault to all sorts of reserve information. The attacker used a fake e-mail to enter Bangladesh Bank's network and made the robbery. Following the Bangladesh Bank Incident, several additional private banking institutions were targeted by cyber-attacks. These scenarios suggest that Bangladesh's cyber security is in jeopardy.

Following is some of the relevant and recent cyber security incidents taken place within some of the world's largest organizations.

- The Google Attack on October 16, 2020  
Google is multinational technology company serving enormous users by services such as artificial intelligence, quantum computing, e-commerce, online advertising, cloud computing, search engine and computer software. The Threat Analysis Group (TAG) of Google informed via posting a blog about how the threats and its participants managed to change its tactics due to the U.S election in the year 2020. During the attack, the attacker spoofed 167

Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers by several networks and had sent numerous responses to them.

- The AWS DDoS Attack in 2020

Amazon Web Services is the provider of highly scalable, dependable, and economical infrastructure platform in the cloud that supports thousands of businesses around the world. In February 2020, it was hit by a giant DDoS attack. The attack was one of the most extreme known about DDoS attack. During the attack, an AWS customer was targeted using the techniques known as Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. The approach depends on endangered third-party CLDAP servers and intensifies the volume of data being dispatched to the target's IP address, the intensify amount is about 56 to 70 times. The period of this attack was longed for three days and lasted at most to 2.3 terabytes/second.

In such circumstance, considering such incidents, this study is an effort and analysis to understand how different Government organizations of Bangladesh are tackling Information Security issues as they deal with sensitive and important data. The selected organizations for the following research are some of the very prime organizations that plays strong roles in the perspective of the country. By means of an interpretive research strategy, the aim of the following research is to investigate exactly how much of the Information Security Governance (ISG) measures are outlined, performed, and formed in several critical organization's infrastructure in Bangladesh. Therefore, the research clearly identifies the socio-technical nature of Information Security Governance (ISG) and pull-out understandings from the Institutional Theory. The purpose is to present a general vision of the security level of Information Systems (IS) in Bangladesh's organizational culture and to discuss the safety protocols that are being grabbed by them. The following research is also attempted to discuss the several Information Security Management System (ISMS) concepts and several ISO Standard protocols. The Government of Bangladesh regulates its initiatives according to the country's needs thus such analytical studies are effective to present a representation of the problem, why and how it is occurring and the necessities that needs to be considered. The documentation can be used for future analysis and implementation of threat identification tools.

## **1.2 Research Problem**

According to observations, practically every element of human life is now permeated with a cyber component. New cyber security solutions, tools, and methodologies must be developed in the context of the fast use of smart mobile terminals in order to safeguard individual and organizational information assets. According to trend analysis, malware assaults on emerging mobile communication networks and terminals are becoming more frequent and sophisticated. Because they have unprotected access to many digital resources, mobile devices are vulnerable to cyber-attacks. Therefore, taxonomies for cyber-attacks would be helpful in examining and evaluating the impact of malware on the operation of mobile terminals and networks. According to the Microsoft Security Intelligence Report 2015 (Volume 20), most malware attempts to infect PCs are rejected before they succeed on computers running real-time security software. It is vital to think about infection attempts that are thwarted as well as infections that are eliminated while analyzing the malware landscape. Malicious actors can employ a variety of tactics to spread mobile malware, and infected devices can then be used as a launch pad for more cyber-attacks. Specially in case of aged people or uneducated people, such attacks can be easily attempted as they are unaware of fake hyperlinks or websites. They tend to easily visit any page or websites that are suggested regardless of the security measures. Malware attacks against smart mobile terminals are particularly complex since they contain a large amount of sensitive data. Mobile phone usage is very common in these days. In order to distinguish between legitimate and harmful behavior, the cyber security community is continually working to evaluate the modes of operation of pertinent malware.

Information Security always denotes to preserve Information commencing illegal entry, practicing odds, modification, perusal, release, commotion, or destruction of crucial data. Such data are in general public data that can be confidential, personal or restrictive such as public wealth, medical history etc. and can be retrieved from the government organizations only. Thus, here Information society refers to the Government organizations only. Moreover, the data can be related to voting data that aggregates public choice and democracy of the nation. Often data are passed or stolen by individuals due to their financial crisis. In addition to that, the influence of information incidents, which consequently precede to loss of data, leakages of critical

information, wasted effort, and the spread of cyber infection can have devastating results towards the nation. In fact, such security threats have serious consequences on public mental health, as a result can also be dangerous towards the society resulting increase in suicidal cases. It has been observed that several cyber security cases have given rise to suicidal attempts conducted by the victims. Information security experts, forensics analyst, network superintendent, sysadmin, coder and software system engineer should be prepared for rapid and unprecedented security threats, train its IT official personnel and equip its organizations with the latest innovations to cope up with the situation and regulate normal proceedings. According to the available research (Jaeger, 2013), lost paper files accounted for 38 percent of data breaches, misplaced portable memory devices accounted for 27 percent, and hackers accounted for just 11 percent of data breaches. In addition, negligent personnel or contractors were responsible for 39 percent of all events, hackers or criminal insiders were responsible for 37 percent, and system "glitches" were responsible for 24 percent. As a result, it is possible to argue that the human element is the weakest link in information security (Poneman Institute, 2012).

With a view to simplify the service render process, overcome the frequencies of such incidents and to proliferation of office productivity, Government of Bangladesh (GoB) digitized its critical information in such a manner that Confidentiality-Integrity-Availability (CIA) of information is intact. When connecting a new request, making a record, or assuring access to approximately information, the CIA standards are one that many societies and enterprises follow. All these safe-keeping regions must lead to a result for data to be completely safe (Mrs. Ashwini Sheth and Mr. Sachin Bhosale, 2021). The CIA triad is the most widely accepted collective standard for determining, selecting, and deploying the appropriate safety panels to reduce risk. Followings are discussed below:

- i. Confidentiality:

Assuring that your complicated data is only accessible to authorized people and that no information is leaked to undesired parties. If your key is private and will not be shared, who will have access to it, which will jeopardize your privacy. Methods to safeguard Confidentiality: Data encryption, Two or Multifactor verification and Confirming Biometrics



ii. Integrity:

Ensure that all of your data is accurate and reliable, and that it does not vary from one fact to another during the program. Methods of ensuring Integrity:

- No illegal should have access to the records, as this violates privacy
- Controls for Operator Contact.
- Appropriate backups must be available in order to return quickly.
- A version supervisory must be there to monitor who has altered the log.

iii. Availability:

There will be no bout alerts such as Denial of Service whenever the operator requests a resource for a piece of statistics (DoS). The evidence must be available in its whole. For example, if an attacker takes control of a website, resulting in a DoS, the website's accessibility is hampered. Few steps of Availability.

- Sorting the possessions into categories based on their relative importance. At all times, the most crucial ones are kept protected.
- Defending against potential risks.
- Choosing the best security guarding strategy for each threat
- Keeping an eye on any data breaches and managing data at rest and in motion.
- Iterative maintenance and addressing any concerns that arise.
- Based on past assessments, updating policies to deal with risk.

The Government of Bangladesh deliberately takes necessary measures to improve its security infrastructure, encourages the people to work on modern technologies to represent the country to the world. Bangladesh is evolving day by day in terms of Standardization, technology, education, and economy and is considered as a developing country. Bangladesh Government has formed an e-Government Computer Incident Response Team (BGD e-GOV CIRT), deliberately serving as the National CIRT of Bangladesh (N-CERT). Their activities include, but are not limited to, collecting, evaluating, and acting to cybersecurity occurrences and actions in Bangladesh's territory. The organization holds collaboration with international organizations as partners to ensure security in cyberspace. The purpose of BGD e-GOV CIRT is also to conduct research and development based on the security threat

issues and encountered vulnerabilities. It reviews and initiates necessary steps to resolve cyber security issues, guides public upon several security threats that are frequently taking place.

BGD e-GOV CIRT also works with various Government Agencies, Critical Information Infrastructures (CII), Financial Organizations, Law Enforcement Agencies (LEAs), Academia & Civil Societies to enhance Bangladesh's cyber security measures and it has a well-built tie with the cybersecurity international organizations and communities. This helps to maintain and regulate trans-border cyber threat issues encountered within the country as a representative of Bangladesh.

In order to create and uphold faith in between management, citizen and business units, the safeguard of information remains crucial and must be handled with great care. Thus, preservation of public documents and information systems in the cyber space are core responsibility of the information owner and custodian of each government agency to stop damage of public and government asset as well as health. There have been several recent incidents of cyber security threats devastating mental condition of the victim, resulting in suicidal attempts. Such impacts the overall community and as a result the nation itself. Therefore, every individual such as a user or any IT official personnel must take necessary measures to ensure data privacy and security.

In addition, Critical Information Infrastructure (CII) refers to government entities which are physical or virtual systems that control, process, transmit, receive, or store electronic information in any form like data, text, image, voice, video and more (wikia.org, 2021). It could be compared with the 'blood diffusion system' of a living body. If negatively impacted, it would affect the national economy and security of a nation. Additionally, it would affect public health, safety, and financial security. So, various updated security controls and protocols are needed to protect critical infrastructures against growing and evolving threats on government valuable information asset. To tighten the security level of the organization's valuable information, risks associated to the employees, processes, devices, and technology must be taken care of and it is necessary to correctly perform the identification of threats. Analysis of the vulnerabilities of the organizational activities which support the fluxes of information. The organization also needs to be proactive to threats and tolerant to malwares or virus. Continuous updating its safety measures to respond to

any recent or upcoming threats. Following is some of the points that has better explanation of why Information security management is important for an organization. Why the society needs proper Information security management in today's world of Information Society? To be very precise, here society indicates the Government organizations only because it is dealing with the confidentiality of data within a government organization.

- Reduction of data infringement and illegal entrance in IT systems of organizations.
- Protecting sensitive and confidential data by restricting user access.
- Prevention of web page disfigurement, dismantling of information, cyber espionage, misappropriation of information, Distributed Denial of Services (DDoS) attacks.
- Reduction of attacks reduces the downtime of any application, as a result increasing the overall productivity of the organization.
- Corroborating continuation of business through data protection and hiding.
- Ensuring mental satisfaction of the citizens by keeping data secured and confidential.
- Smooth running of Government services with secured data transfer and maintenance of restricted, confidential, and private data. As a result, smooth running of the government policies.

### **1.3 Significance of the Research Problem**

Information Security plays a vital role and can have serious effects in many of the cases such as jobs, finance and economy, commerce, security, law and other situation like, health-nutrition, education, strategic plans, resource efficiency and much more sensitive information. The Government Organizations of Bangladesh has the access to National database thus such organizations are prior to cyber-attack and information security is very important towards such organization. Information Security is a term that is important for both Government and Non-government organization, but this research focuses on the Government Organizations only. Online business organizations can have severe impact due to negligence of Information security. Identity theft, data breaches, and other online scams are lethal to online commercial enterprises, so information security management is a top priority. It has been analyzed

that in UK about 93% large organizations and 87% of small companies suffered from breaches of data (Zahoor Ahmed Soomro and Mahmood Hussain Shah, 2016). As the security landscape evolves with new threats cropping up almost daily, Information security professionals face hurdles to keep pace with security offenders as offenders try to show up with new and distinct approaches. In addition, data breaches or security defaults can result in decrease in number of users of the organization. They are likely to face massive challenges as it cannot be predicted very easily of who is the next target and what is the process but at the same time, if understood, analyzed, and handled well, it may offer us huge opportunities to minimize the impact. Moreover, the COVID-19 pandemic period has given the cyber criminals a wide range of scopes due to sudden lockdown throughout the world when all the offices remained closed, necessary security measures were not considered at all. Such occasions are of great interests of the cyber criminals as during such period, it is very easy to get access to any system due to lack of maintenance, updates, and usage. In addition, the pandemic resulted in greater usage of technology or can be said as made people technology dependent for various jobs such as money transfer, paying bills, fees and etc.

An increasing acknowledgement can be observed in the academics [Straub, Goodman & Baskerville 2008, Baskerville & Siponen 2002; Dhillon 2007;] and the dedicated research paper [DTT 2007; ITGI 2008] for last couple of years that technical clarifications are essential but not appropriately enough for facing Information safety encounters. It has changed focus from seeing Information Security as a working obligation apprehensive with procedural structure of an institution based and tactical business-led accountability introducing more importance on professional necessities, skilled employee, tools and keeping important information assets (Allen & Westby 2007 and Ernst & Young 2009). Major hurdles to successful information security, according to respondents in a global information security study, are a lack of top management support, budgetary limits, a lack of skilled human resources, and a lack of tools. Management is responsible for overcoming these challenges, with top-level management playing a key role. As a result, information security managers are ought to take a more all-encompassing approach to information security, which should include top management engagement from e-tailors. Furthermore, organizational variables like industry, size, and structure have a substantial impact on information security management adoption. Large financial firms are more sensitive to the

effectiveness of information security management due to the increased risk of security assaults. In addition to developing an information security strategy, management support is required for the policy's effective implementation.

There are some traditional principles, doctrinaire contexts, frameworks and prototypes which framed to contribute overriding information security, but no single particular outline has been accepted commonly. Whereas the encounters of Information Security are widespread in relation to shielding information assets, the means by which an institution reacts might differ with its exact perspective, necessities and threat resilience altitudes. Information security rules have a big impact on the security of information systems and the smooth running of businesses. As a result, the human aspect in information security management cannot be overlooked. On the other hand, Information security cannot be efficiently maintained or managed with a single scope, rather multiple domain scopes must be considered for information security management such as human aspects- Human resources, including such organizing, acquiring, inspiring, training, simulation, and managing human activities in organizations, as well as managerial responsibilities such as overseeing, controlling, making decisions, and monitoring security management policies, are all examples of job roles.

There are inadequate experiential studies pointed at how the aims of those principles and contexts are basically attained in institutions (Siponen 2006) and synchronized with other practices. Several decentralized decision systems are also advocated for effective information security management. Moreover, additional conceptualization on exactly how Information Security is incorporated in organization and its interior and exterior effects is essential. It has been recognized as particularly significant for the arrangement of Information Technology assessments (Love et al 2010).

The development of information security technologies is insufficient to prevent fraudsters from interfering with data. Cyber criminals are actively working to introduce random techniques. The efficiency of an information security governance program and policy is determined by the quality of executive management support, continuous reviews, and the inclusion of specific adjustments to address new difficulties (Zahoor Ahmed Soomro and Mahmood Hussain Shah, 2016). With this

background, this research is very much relevant for contemporary Information Security analysis as well as development issues.

#### **1.4 Scope of the Study**

There is a wide variety in understanding and meanings of the terminology ‘Information Security’ (IS) are prevailing in research papers. For instance, the Information Technology Governance Institute (ITGI 2006) describes IS “... subset of governance and management that offers strategic vision, assures that goals are met, manages risks correctly, makes responsible use of corporate resources, and tracks the successfulness of the organization security plan.” In book chapters, the definitions lie as Security refers to both the state of being safe and free from harm, as well as the activities performed to make someone or something safe. Policy, education, training, awareness, and technology are all used to ensure the confidentiality, availability, and integrity of information assets while they are being stored, processed, or transmitted. Information security is crucial for government organizations since the government entities in Bangladesh have access to the national database, this makes them vulnerable to cyberattacks. Both government and non-governmental organizations should be concerned with information security, however this study mainly addresses government organizations.

Von Solms (2006) and McFadzean, Ezingard & Birchall (2007) identify Information Security a part of organization’s IT procedures or comprise features of control and label its effort within the domain of Information Security Management Systems (Dutta & McCrohan 2002; Caralli 2004). Apart from this, Thomson and von Solms (2006) opined Information Security as having an overlying task within institutional control as well as office norm, accepting the terminology “information security obedience” with a view to replicate its affiliation among all three arenas.

Therefore, collective denotation of IS seems remain common in range and to conglomerate Information Security with present ideas of organization and IT procedures. Basically, scope denotes to periphery limitations in a theory submission (Bhattacharjee, 2012; Denscombe, 2013). This research purpose was to perceive Information Security Governance practiced at Bangladesh government organizations and contribute to tactical and strategic level managers for further augmentation of innovative and standard IS programs. This research is dedicated upon exploring the

height of up to which level IT experts of government offices execute strategic adjustment and policies, capital & crisis management, significant use of value delivery and performance measurement in producing effectiveness of existing protection mechanism that checks and prevents critical information security breaches and minimizes information leakage. In addition, their efforts add towards human resource capability in information security management.

### **1.5 Objectives of the Study**

What the research aims to achieve:

- To identify most pertinent information risks, threats and vulnerabilities that usually takes place in some important Bangladesh Government leading organizations (e.g., Bangladesh Bank, Election Commission, CID/SB of Bangladesh Police and Land Records and Survey Department etc.). Such organizations contain important public data that are confidential, private and restricted. Any attempt to manipulate the data of these organization will have serious impact on the nation and wrong evaluation of result.
- To get a deep understanding of incidental impact and consequences of several information threats in public enterprises, what measures are taken by them during the threat attacks. The category of the attack and its frequencies, analysis of its target. Finally, the overall effect of the encountered attack.
- To examine the results of existing protection mechanism applied in those important Bangladesh Government leading organizations by analyzing its effect rate and through the interview session; and
- To provide fresh insights into best practices appropriate to handle these incidents in a very efficient manner, analyzing the threat patterns and reports for possible future attack management in a sufficient manner.

It is undeniable that Bangladesh's cyberspace vulnerability is growing by the day. To cope with the circumstances as well as competition, new technologies and services must be introduced to lessen the impact. To combat cyber-threats, technological and legal progress is required. To prevent cybercrime, it is also vital to raise awareness among internet users. Cavities in secure online activities can be reduced with proper precautions and prompt correction.

## **1.6 Research Questions**

Taking all these things into consideration, the effort has been dedicated to find out the answers to the following questions:

- Which are the major threats evolving in government Critical Information Infrastructures (CII) and how do they affect the organizations? What is the type of attacks encountered and their details?
- What are the significant security measures adopted to protect sensitive government information? and
- How those threats could be minimized in public information domain protecting the organization value?

## **1.7 Limitations of the Study:**

Limitations echo possible research flaws (Bhattacharjee, 2012 & Brutus et al 2013). The interview reply rate during conducting the research was awfully small as this study is sensitive in nature, contains sensitive government organization data. Leakage of such important and sensitive data has serious consequences. Earlier survey-based study proof revealed that the researcher may experience very little response rate while collecting data through interviewing on sensitive subject (Flores, Antonsen, & Ekstedt, 2014; Yaokumah, 2013). The scope of this report is based on a very few [04 (four) only] organization of Bangladesh government. Not necessarily, it represents all public critical information infrastructure of Bangladesh. The respondents are mostly IT management staffs of the concerned offices those who are connected to security threat attacks and management. The research took place during the pandemic of COVID-19, when the world seemed to have stopped every of its activities and execution. Therefore, there are limitations to perform face to face interview with a good number of organizational employees as the Covid-19 situation has been worsening. It is considered that face to face interview helps to observe interviewer's expressions and helps in asking few more questions. Moreover, it is also because of their different organizational culture of the selected government offices, the answer to same nature semi-structured interview question may not be as same as it is expected. So, it is very difficult to generalize them although reliability and validity of data that have been observed.



As the topic is huge and associated by a wide variety of persuasions and analytical data, therefore, it was a challenging task to determine an outright resolution. A lot of ambiguities are there for accomplishment of the detailed solution. Moreover, interview data taken from institutes had many query marks. The absence of some convinced information and security resources from dispersed sources has operated as an excessive hurdle and time compelling therefore interview studies can be both expensive and time-consuming to conduct. Pulling out of information from the government people of different strata was not helpful at all due to lack of IT knowledge and biased thinking. It is observed that some of the officials have very little IT knowledge thus appropriate results cannot be obtained. Biasness might arise as a result of an interview, the respondent's responses might be influenced by his/her reaction to the interviewer's race, class, age for example- Many respondents are concerned about the lack of anonymity in interview research. Nevertheless, it was due to pandemic situation, that most of the offices was out of reach and respondent were reluctant to response carefully, there lies a problem of accessibility to respondents. So, these are some limitations of the study that made it difficult to conclude.

The COVID-19 situation resulted in difficulty upon carrying the research necessities, but this opportunity had been widely used by cyber security criminals upon achieving their goals.

### **1.8 Justification of the Research**

The outcome of the study will be valuable for understanding national risk perspectives. It will help the Government to look onto issues that must be taken care of, work on the weak scopes to improve security management process. It will contribute to review or readjust the National Strategy for Robotics, National IoT strategy, National Blockchain Strategy, National Strategy for Artificial Intelligence, Government e-mail Guideline 2019, Information Security Policy Guideline 2014, National Cyber Security Strategy 2014, Digital Device, Internet and Information Security Manual 2020, Guideline on ICT Security 2015 (for Banks and Non-Bank Financial Institutions) and other ICT manuals practiced in several government organizations. Government has already taken great initiatives in such concerns, but these research observations can help look forward in details about the necessities to be performed. Government will be benefited by the analysis results and directly act upon

execution to enhance their current way of working. Develop and implement high accuracy framework for the security management system of an organization.

Furthermore, the findings of this research work might help government enterprises' IT staffs to improve their awareness on IS with a view to shield information assets more effectually along with simultaneous saving in regaining costs. CEOs, CISOs, Risk Assessors, IT Auditors, Security Experts, System Analysts might be benefited and feel encouragement for managing Information Security in their relevant domain. The statistical data related to the research will also help organizations to observe the attack criteria and frequencies, their impacts and consequences and will encourage them to acquire proper security management measures to tighten their data security. Lastly, the preserving of confidential, restricted data will enable a nation to grow confidently as public data are precious as well as very important in maintaining economical state of the country. Every individual has some important data that must be handled with great care. In economics, data is crucial since it explains and measures the challenges and problems that economists are attempting to comprehend. Economic and social data are published by a few government bodies so proper initiatives must be acquired to stop data misuse and breaches.

### **1.9 Structure of the Thesis**

This research paper has been organized as follows- the first chapter set the contextual of the study, study objectives, precise exploration questions and a brief description of justification of the study. The second chapter basically dealt with Literature Review. It also shows the role of various internationally accepted standards. The Third Chapter is about Theoretical Framework of the paper. Five relevant theories are mentioned here. It also stated the Conceptual Framework that guided much of the subsequent materials of the dissertation. Chapter four showed on Methodology of investigation, various implemented methods and their relevancy in research context, sources of data, analytical methods and reliability level of empirical findings. The next chapter revealed current status of Critical Information Infrastructure and emerging challenges which are causing concern through a rigorous analysis. There is a qualitative assessment of the interview data both from the respondents and the key informant in this chapter. It also marks the major findings from the analysis. Chapter six contains discussion on security issues and at the same time put lights on ways forward. The last

chapter summarizes key points and issues that emerged from the preceding chapters. Finally, there were some specific recommendations to mitigate the loss. The paper ends with some indication for future research.

## **CHAPTER II: LITERATURE REVIEW**

### **2.1 Overview**

Jaffe & Cowell, 2014 argued that a researcher achieves perception within a particular subject matter while accomplishing an early academic literature assessment in numerous means. A literature review is an examination of academic sources on a particular subject. It gives the researchers a broad perspective of the body of existing knowledge, enabling them to pinpoint pertinent ideas, strategies, and research requirements. Locating pertinent works, analyzing them critically, and summarizing what is learnt are the steps involved in writing a literature review. When reviewing literatures, the purpose should be rebuilt significant added knowledge within a certain topic field (Schryen, 2013). Thus, a review of literature denotes the initial essential footstep in reconstructing the collected information and predominantly delineates rebuilding into the following literature study (Wahl & Bull, 2013).

There is enormous literature on Information Security Management and a lot of frameworks, policies and ideas have been contributed till now, some of which has been discussed in the paper. Since this research broadly focus on Information Security practiced in Government organization, more concentration has been paid to the literature pertinent to socio-technical aspects which are considered relevant with Bangladesh Government laws, rules, circulars and regulations. The policies followed by the organization and their security plans towards cyber security threats have been obtained via an interview session and showed as an observation. There is also an effort to investigate the features and topics that really influence organizational Information Security culture development and deployment, encouraging them to put more effort on their information security management system.

### **2.2 Information Security Management Systems (ISMS)**

Information Security is something that is achieved by limiting the impact of security incidents, information security aims to ensure company continuity and minimize corporate harm (Von Solms, 1998). As seen below, information security can be characterized in a variety of ways. An organization's approach to information security and privacy is described and shown through an Information Security Management System. It will assist it in identifying and addressing threats and opportunities that

may exist in relation to the important information and any associated assets. This safeguards the company from security breaches and protects it from disruption if and when they occur. Information security is defined by the international standard ISO/IEC 27002 (2005) as the preservation of information's confidentiality, integrity, and availability (ISO/IEC 27002, 2005, p. 1). Information can take numerous forms in the context of ISO/IEC 27002 (2005). It can be printed or written on paper, kept electronically, sent by mail or electronic means, exhibited in films, discussed, and so forth (ISO/IEC 27002, 2005, p. 1). Information security, according to Whitman and Mattord (2009), is "the safeguarding of information and its key elements, including systems and networks." The purpose of a foundation's ISMS is to offer easy entrance and ensure CIA aspects of Information. Traditionally, the industry standard has been to ensure the confidentiality, integrity, and availability of information, often known as the CIA triangle in information security. Security of these three information qualities is as critical now as it has always been, but the CIA triangle model no longer appropriately reflects the computer industry's continuously changing environment. The features or characteristics that secure information should have been widely used to define information security. These normally include information secrecy, integrity, and availability, but they can also include other attributes. Managing those concerns of information in the Government offices have different significance than any other private owned office as Government offices holds on important jobs and data that is a prior concern. These refer to a wide variety of important perspective of Information Security Management.

There is a very common concern regarding Information Security Management System. Why does an organization require ISMS? An organization will not be able to achieve ISO 27001 without an ISMS. It's an important aspect of the certification and compliance procedure. This is because it reflects how the company handles information security. It specifies how the company detect and respond to opportunities and dangers posed by the organization's information and assets. It is the only way to demonstrate that the company is correctly managing their information security is to have an information security management system in place. Some of the key points regarding ISMS is given below:

- Protect the information assets of the company.
- Make it simple to show how secure the data is.
- Demonstrate how seriously the company takes data security.
- Assist the company in staying on top of new data security threats and possibilities.
- Assist the company's development and expansion.

The second concern regarding Information security management is what are the advantages of an ISMS for a company? The answer to the question is: An efficient ISMS can assist a company in a variety of ways. This is especially true in today's threat-heavy environment, when strong data security is a must in many supply chains. Weak data security encourages cyber threat attacks. Small businesses are especially vulnerable to data leaks because they might jeopardize their most valuable assets: trust and reputation. Poor data security is almost always to blame.

### **2.2.1 ISMS Concept**

An ISMS enables a company to run its information security management system in a methodical manner. By developing the ISMS, a company may determine the appropriate security level, formulate plans, distribute assets, and manage systems based on its own risk assessment as well as individual technical countermeasures for each issue. "Preserve the confidentiality, integrity, and availability of information through the application of a risk management approach and provide interested parties confidence that risks are adequately addressed," according to the ISMS' core premise. To accomplish this, the ISMS must be incorporated into and part of the organization's processes and broader management structure. The CIA properties of Information reinforce security services. Supplementary properties like non-repudiation, accountability, reliability is also well encompassing with it. In this paper, ISMS is explained with confirming business continuity and reducing damage by avoiding and decreasing of security events.

The plan-do-check-act (PDCA) cycle is frequently used to structure ISMS procedures. The PDCA cycle (Plan-Do-Check-Act) is a participative problem-solving technique for improving processes and implementing change. The PDCA cycle is a continuous

improvement strategy and is a continuing feedback loop for iterations and process improvements, rather than a one-and-done procedure. Teams build hypotheses, test those hypotheses, and improve on them in a continuous improvement cycle by following the PDCA cycle. The PDCA cycle is an effective method for addressing, analyzing, and resolving business issues. The PDCA cycle provides flexibility and iterative improvement because it is based on the continuous improvement process. The phases of the process are:

- PLAN: ISMS planning
- DO: ISMS development and operations
- CHECK: ISMS verification and validation
- ACT: ISMS maintenance and enhancement.

General conception on Information Security has changed from genuinely mechanical in the 1970 to recent conventional character in public offices. From ancient point of view, von Solms, 2006 argued that the evolvement of ISMS methodology over the last five decades categorized by 04 (four) division, those are- mechanical wave (up to early 1980s), executive wave (from early 1980s to mid-1990s), Official wave (stated in late 1990s) and Supremacy wave (exists till today). Each wave defines general approaches to its management for the certain time duration.

Contemporary research on ISMS carried out at micro level has been identified relevant factors of Information Security on organizations basis (Dhillon, 2011). The author argued that external nets might not intrinsically protect. So, optimal care was needed for the diverse phases of inside security system.

### **2.2.2. ISMS and others standard and guideline adaption in the Public Sector**

The Cyber Security Baseline Standards' principal purpose is to increase the resilience and security of public sector information and communications technology infrastructure and systems (ICT). The rise in government and citizen concern about data security has resulted in more complicated security needs, which frequently involve the integration of numerous approaches. Combination of multiple approaches integrates the benefits of multiple approaches resulting a better solution. As a result, modern information security deployment has become even more difficult, particularly

in government information technology procedures. Managerial information technology practices are the driving force behind IT effectiveness. Information technology is used in a variety of ways by management. To ensure compliance with regulations in the public sector, a process of integrating security practices into public sector firms and their activities should be considered.

It is high time to adopt best practice and international guideline to protect public ICT infrastructure, ISO 27001(ISO guideline that outlines how to manage information security in an organization, with the goal of assisting organizations in defining, implementing, operating, controlling, and improving information security using a risk-based approach.), the leading ISO standard for information security management. ISO 27001 is one of the most widely used standards in the ISO 27000 series. It's a process management and assessment standard that lays out the requirements for an information security management system (ISMS). The requirements for adopting, maintaining, and upgrading an ISMS are outlined in the first part of this standard, while the control objectives and security controls are described in annex A. Annex A lists a variety of information security controls and other measures. ISO 27001:2013 updates ISO 27001:2005. Annex A of the 2005 standard has 133 controls in 11 categories, but Annex A of the updated version has 133 controls in 11 categories (Shojaie and Federrath, 2015, Shivashankarappa and Smalov, 2012, David and Fbes, 2010). The ISO 27000 series includes more than only ISO 27001. ISO 27002 is another ISO 27000 series information security standard that contains rules that should be implemented with the ISMS. ISO 27002 is connected to ISO 27001, with an ISO 27001 Annex listing ISO 27002 controls.

- ISO 27000 – ISMS – Overview and vocabulary.
- ISO 27003 – ISMS implementation guidance.
- ISO 27004 – Information security management – Measurement.
- ISO 27005 – Information security risk management.
- ISO 27006 –Requirements for bodies providing audit and certification of ISMS.
- ISO 27007 – Guidelines for ISMS auditing.
- ISO 27008 – Guidance for auditors on ISMS controls.
- ISO 27010 and following – sector specific standards.
- ISO 27030 and following – standards for technical controls and guidelines for ISO 27002.



COBIT (Control Objectives for Information and Related Technologies) is an ISACA framework for managing and governing information technology (IT). The framework is business-oriented, defining a series of generic processes for IT management, each with process inputs and outputs, important process activities, process objectives, performance measures, and a basic maturity model. Common Objectives for Information and related technology COBIT (COBIT is suggested for businesses that rely on technology to offer relevant and accurate information, as well as for those who provide information and information technologies that must meet specific quality, dependability, and control requirements.) an IT management and governance framework.

The Special Publication (SP) 800 series of NIST publications contains material of relevance to the computer security community. The series includes NIST's cybersecurity guidelines, recommendations, technical specifications, and annual reports. SP 800 publications are designed to address and assist the information and information systems security and privacy needs of the United States Federal Government. NIST publishes SP 800-series papers according to its legislative obligations under the Federal Information Security Modernization Act (FISMA) of 2014. The NIST SP 800 series (provides standards for the implementation of computer security policies, procedures, and configurations) is a set of documents about computer security produced by the US government. Every standard has some similarities and differences, it can be used together during an information security implementation in the public sector to improve information protection. Combination of the standards tends to multiply the advantages of the standards producing a fruitful outcome.

SOX (Sarbanes–Oxley) and EU GDPR (European Union General Data Protection Regulation) have different goals and need different activities to secure information in terms of legal obligations. The Sarbanes-Oxley Act of 2002 was passed by the US Congress on July 30, 2002, to protect investors against dishonest corporate financial reporting. The SOX Act of 2002, also known as the Corporate Responsibility Act of 2002, demanded significant changes to existing securities laws and placed heavy new penalties on those who broke them. The Sarbanes-Oxley (SOX) Act's main points:

- The Sarbanes-Oxley (SOX) Act of 2002 was enacted in reaction to many high-profile corporate financial crises that occurred earlier in the decade.
- The act established tough new restrictions for accountants, auditors, and company officers, as well as new recordkeeping obligations.
- In addition, the statute imposed new criminal penalties for securities law violations.

The GDPR applies to a corporation or entity that processes personal data as part of the activities of one of its EU branches, regardless of where the data is handled; or a company based outside the EU that offers goods or services (paid or unpaid) or monitors the behavior of EU citizens. One must comply with the GDPR if the company is a small and medium-sized organization ('SME') that handles personal data in the manner outlined above. Some GDPR responsibilities, such as the appointment of a Data Protection Officer ('DPO'), will not apply if processing personal data is not a key element of the business and the activity does not pose a risk to persons.

Frameworks like COBIT and ITIL have diverse approaches to information security when it comes to information technology procedures. The public sector should tailor these guidelines and frameworks in the Bangladesh context. Integrated frameworks help cope with complexity.

Information Systems Governance (ISG) is a collection of regulations that allows executives and stakeholders to select how they will manage their information systems. ISG System in government domain is important as the external agents of electronic governance system is required to handle cautiously. In addition to that, public domains are equipped with the upcoming plan, policies, strategies, frameworks, and a wide variety of valuable national archives. Any violation of those critical informational aspects may cause severe damage to the country as well as its citizen.

### **2.2.3 Role of Various Standards**

A good number of Standards have been practiced by various independent international and government institutions with a view to protect managerial security in a general manner and according to their choices.

Recent surveyed literatures mostly have disproportionately concentrated upon the mechanical aspect alone. Its partiality could be absence of information regarding

the compound and versatile landscape of Information Security system or for the diverse opinions on information security glitches from diverse viewpoints. While practicing, corporate offices showed that their organization security hitches also call for administrative, societal, moral, and lawful solutions.

For Bangladesh case, it would not be exaggerated to say that there are a very few literatures on government information security system whereas the Government information should have the highest of the priority. The literature review did not define any study that diagnosed integrated structures or pronounced a perfect paradigm or framework screening all the aspects which support the enactment and acceptance of Information Security accomplishment or maintenance.

In this regard, a good number of extensively prescribed governance structures available to monitor institutions in framing and effectively functioning their ISMS endeavors. One of the renowned such frameworks is ISO 27K series. In the context of an overall Information Security Management System (ISMS), which is modeled after quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series), and other management systems, the series provides best practice recommendations for information security management—the management of information risks through information security controls (ISMS). Intentionally broad in scope, the series addresses concerns beyond those of privacy, confidentiality, and IT/technical/cybersecurity challenges. It can be used by businesses of any size or shape. All companies are advised to analyze their information risks and then treat them appropriately (usually through information security controls), considering the guidance and ideas provided. The ISMS approach includes continual feedback and improvement actions to respond to the random nature of information risk and security. Continuous feedback system and improvements enhance the existing the approach and develops more active system.

This research is heavily based upon most popular Global Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013 that could be considered as the best international standards governing information security in organizations. ISO/IEC 27002: Guidelines for organizational information security standards and management practices are provided in 2013, covering control selection, installation, and upkeep while taking into account the organization's information security risk environment (s).

The ISO/IEC 27002 safety purviews are (ISO/IEC 27002, 2009):

1. Safety strategy – exhibits administration’s obligation to and maintenance for information security. The strategy followed by the administration to minimize threats and overcome attacks. Might be usage of various software to protect the system from malwares or viruses.
2. Arrangement of Information Security – develops configuration for the synchronization as well as execute of Information Security in the workplaces, execute setups and continuous updates. It allocates Information Security accountability among the employee hierarchy.
3. Resource supervision – accomplishes a register and cataloging of entire acute or vital information properties. Supervision of the vital resources to enhance the monitoring of the changes.
4. Personnel security – accomplishes the safety phases connected towards workforces, with a view to decrease the chance of mistake, stealing, scam, or misappropriation of PC resources by endorsing employee training and sensitizing about the vulnerabilities and intimidations to information. Regular basis of employee training for self-awareness and making them understand the importance of the data that they handle. It can be setting difficult password, changing passwords at times, not revealing data to anyone-not even the family, and ensuring that the data is kept hidden or protected. Employees without knowledge about the importance of data often result data stealing or scam so employees must be well trained about the measures that they should acquire to protect the data they are handling.
5. Industrial security – The protection of manufacturing and industrial plants from flaws, whether deliberate or unintentional, is referred to as industrial security. Information technology (IT) used to manage security in the form of IT security. Using information technology, today's production and industrial units are also extremely networked. In addition, safeguards data transform services, with a view to avoid unapproved admittance to critical information.

6. Transmission and Business processes – Control mechanical safety in networks and systems, to decrease the possibility of disaster and its magnitudes and improve occurrence reaction techniques. The control in mechanical safety in networks will help minimization of the spread of the virus (threat) throughout the system. As a result, less damage leads to faster recovery due to improving occurrence reaction techniques.
7. Accessibility control – Restrictions on entrance permission into nets, server systems, apps, utilities, and documents for unlawful accomplishments. The system or the server is the main hub for the data management therefore, authorities must impose strict restrictions in entrance and usage to such ends. This will reduce the frequency or rate of being attacked by a threat. High official personnel must only have access to such ends so that easy access can be denied.
8. Information systems purchase, improvement, and preservation – inhibit from the damage, alteration, or mismanagement of information in OS and apps software. Must be regular in updates and usage of latest versions. Latest version or updates contains solution of some bugs that remained in the immediate previous versioning. Therefore, helps the system to protect from such loopholes.
9. Information security event control – Reacts properly to Information Security break that was committed by a hacker. Quicker reaction results in less damage of the overall asset whether it is only the data or the wealth. Early recognition of the threat results in quick reaction towards the threat that has been committed by a cyber security criminal. Proper reacting to events in more and prior important than quick reaction. Proper reaction leads to corrective identification of the imposed threat.
10. Ensure business continuity – Advances the institution's capacity to response quickly to the disruption of precarious actions resulting from system or power failures, untoward incidents, natural disasters or devastations. If the system remains off for a long duration, the economy is affected as well as the continuation of the business remains at stake. Therefore, institutions must make themselves all time

prepared for the rapid threats and respond quick to the attack and resolve the problem. This reduces the proportion of disasters and devastations of the system, overall protecting the system data.

11. Compliance – Confirms that all acts and guidelines are in line with Information Security policies, standards, laws, and regulations. Re-checking of all the previous acts and ensuring their implementation to preserve the information security and enhancement of the information security management.

As already stated, this framework also recommends Plan-Do-Check-Act (PDCA) cycle of Deming. Such quality control framework demonstrated its appropriateness over the past years. However, the standards and access controls mentioned in it have got older by this time. Cyber criminals are always coming up with new trends in their attacks, making it difficult for the older version frameworks to work accordingly. Their effort towards attacking in systems has been consistently increasing. As cyber criminals are promptly become more sophisticated with their intrusion procedures the current state of security processes could pose an increase threat to the organizations. Therefore, the overall organization's value is at stake.

A stakeholder based 'e-Government Master Plan for Digital Bangladesh' has been formulated by ICT division of MoPTIT in 2019. The government of Bangladesh's slogan, "Digital Bangladesh," was particularly important for national growth and had led through several achievements. Vision 2021, or Digital Bangladesh, was a major drive for the country's usage of digital technology. Despite various bottlenecks and limits, work on the realization of Digital Bangladesh was underway. A few digitalization projects have been completed, and many more are still in the works. The country is currently reaping the benefits of digitization in a variety of fields, with over 12 crore mobile clients and 4.3 crore Internet subscribers. The goal was to increase digitalization wherever possible in order to bring more and more services to people's doorsteps. Here are a few examples of available digital services: A few examples of available digital services include registration for academic institutions, publication of test results, registration for jobs abroad, registration for pilgrimages, gathering of official papers, online filing of tax returns, online tendering, and so on. Thanks to online banking networks, the country's financial activities have been accelerated. SMS services for filing police station complaints, online utility bill payments, rapid

communication with people working overseas, and e-passports are just a few examples. Telemedicine, videoconferencing for medical treatment, and videoconferencing for administrative tasks are just a few of the e-services offered in rural Bangladesh. The establishment of approximately 5,000 Union Information Service Centers is a significant boost for Digital Bangladesh, particularly in rural regions. In the recent past, important achievements include the conversion of 8,000 village post offices and around 500 upazila post offices into e-centers, as well as the introduction of mobile money order and postal cash cards. Revolutionary additions include Union Information Centers, District Information Cells, and a National Information Cell. There are a lot more developments coming along the pipeline. A huge range of e-services are provided to rural clients through Deputy Commissioner (DC) Offices in districts and UNO offices in upazilas. Direct digital services cut out the intermediaries, saving time and money. The cities and towns would have become difficult to live in if such online services had not been available. Bangladesh has led to tremendous developments over the last years through the great initiative of the Government.

In addition, this plan is supposed to nullify adoption of similar type of IT projects resulting in a significance reduction of resource wastage. This plan describes the immediate transference from a preventive-based security structure to a wider information security management framework. This framework is a hub on the balance between preventive and responsive initiatives through the organizational security arrangement. This master plan also addresses e-Government related legal frameworks and Information Security related governance issues. The ICT policy of 2009, 2015 & 2018 were elaborate and well-designed plan that directing agencies to the realistic path of digital transformation of the Bangladesh government with a view to deliver effective, suitable, and obvious services to people and industries. Although, basic security measures were addressed, more advance solution like intrusion prevention system, file encryption and vulnerability management systems, data breaches prevention are not stated there. Therefore, the step next towards Government's development is the information security management system as the developed applications during the "Digital Bangladesh" era consists of several public data, some of which are restricted, confidential, and private. This vital information should be handled with extreme caution for the prevention of data breaches, scam, intrusion,

DDoS attack, phishing, and ransomware. Phishing assaults and virus distribution are frequently carried out via websites. The deceptive method of sending emails that look to be from reputable businesses in order to persuade recipients to provide sensitive information like passwords and credit card numbers is called phishing. Even to experienced computer users, rogue websites sometimes appear perfectly legitimate and provide no apparent indicators of their harmful character. These are frequently trustworthy websites that have been compromised by malware, SQL injection, or other techniques so that attackers can profit from the confidence that users have in them. Information leakage in any of the government applications may have serious impact for the citizens as well as the economy and the nation- the results can be devastating and destructive as well.

On May 2015, Bangladesh Bank published the Guidelines on ICT security for Banks and Non-Banks Financial Institutions (NBFIs). According to the guideline, in recent years, the banking industry has transformed the way it provides services to consumers and processes data. This historic change has been brought about by information and communication technology (ICT). Electronic banking is getting more widespread, which is increasing financial inclusion acceptance. As a result, financial institutions' information security has become increasingly vital, and it is critical for us to ensure that risks are effectively detected and controlled. Banks and non-bank financial institutions (NBFIs), as well as their clients and stakeholders, value information and information technology systems. The services that bank and non-bank financial institutions (NBFIs) provide to their customers rely heavily on information assets. The preservation and protection of these assets are critical to the organizations' long-term viability. Analysis reveals that an uptick in cybercrime that has harmed financial institutions' goodwill and economic growth, either indirectly through a loss of faith in digital infrastructure or directly through fraud and extortion in both emerging and established countries. This document suggests that cyber risk is also pertinent with finance, insurance and banking systems that need to be run with high thoughts and endeavors. The guideline advises for security auditing and testing on regular basis. Regular basis monitoring and testing helps in detecting a fault in a system, the fault can be a malware. Early findings of any unusual will help prevention of damage of the system.



The Computer and Information Security Standards is a publication (published in October 2011) of The Royal Australian College of General Practitioners. The Standards are intended to help general practices and other office-based organizations achieve their professional and legal computer and information security duties. It must be mentioned that Computer and information security are not optional: they are a professional and legal prerequisite for using computers in information society. This workbook argues that third party (contractors, vendors and partners) control should be a key focus area for government organization's vital information. The society of government organizations particularly holds access to private data and has a storage of such confidential data. Other organization barely has access to such private data. Government organizations need to make sure a sufficient and suitable level of Information Security with third parties. Office key personnel can be trained to handle sensitive data, prevent from data manipulation, additionally, office machines can be virus-protected through installation of software or information security management policy attained by the office. But government organizations that work with third party must ensure that the third party with whom they are working acquires safety measures as well. The protection is not limited to themselves instead depend on the parties that they have been working on. Leakage of data or any sort of attack can be encountered from third party side as well. Therefore, it is important to ensure information security establishment in third party side as well.

Following international standards and guidelines are in place and adopted worldwide in concern of information security implementation in the public and private sector. The public or private sector relies on any of these to protect their crucial data.

**ISO 27001:** [ISO/IEC 27001](#) is an ISO (International Organization for Standardization) international standard that specifies how to develop and manage an Information Security Management System. One of the ISO 27000 series most often utilized standards is ISO 27001. It is a standard for process management and evaluation that outlines the conditions for an information security management system (ISMS). It offers a library of 133 security measures and the freedom to deploy only the controls that are required, which together form a respectable foundation for cybersecurity (based on risk assessment). However, its most crucial feature is that it creates a management framework for controlling and leading security concerns; as a result, security management becomes a part of an organization's entire management.

As a result, it's feasible that not only better control methods, but also all better managerial practices related to information security would make it more efficient and aligned with business goals. As a result, information security managers should adopt a more holistic approach to information security management that incorporates improved management methodologies. Thus, this standard is a leading information security standard.

**COBIT:** COBIT is an ISACA (Information Systems Audit and Control Association) framework that focuses on enterprise IT governance. It is unique in that it represents the key role that information technology plays in today's enterprises. Enterprise IT governance (GEIT) refers to assuring and enabling information technology and related support, as well as supporting enterprise strategy and achieving enterprise goals. GEIT also makes it possible for the company to meet its regulatory requirements. As a result, GEIT is an integral component of an overall enterprise governance strategy. It is founded on the concept of risk management and managing IT-related hazards at an acceptable level, as do other frameworks; nevertheless, possibly its most important aspect is that it establishes a direct link between a company's strategic goals and its use of technology. Risk management is necessary for lowering the level of risk. Keeping IT-related risks under control allows the firm to respond to attacks more quickly and avoid further damage.

COBIT components are listed below:

- Framework: Groups IT governance goals and best practices into IT domains and processes and connects them to business needs.
- Descriptions of the processes: Everyone in an organization can use a reference process model and a common language. The processes correspond to the areas of responsibility of plan, build, run, and monitor.
- Govern objectives: Provides management with a comprehensive list of high-level requirements to examine in order to effectively control any IT process. Management is responsible for monitoring the whole process and its progress.
- Guidelines for management: Assists in the assignment of responsibilities, the agreement of objectives, the measurement of performance, and the illustration of interrelationships with other processes.

- **Models of maturity:** Assesses process maturity and competence and provides guidance on how to close gaps.

**NIST SP 800 Series:** The National Institute of Standards and Technology publishes the [NIST SP 800](#) series, which includes over a hundred IT security publications. It is perhaps the most complete collection of best practices publicly available, and it is mostly focused on technical security challenges, akin to PCI DSS. Because SP 800 is a collection of documents rather than a single document, it cannot be used as a single framework for implementation; however, NIST SP 800 publications are essential for the implementation of single controls or specific areas of information security. The NIST SP 800 series (which establishes standards for the implementation of computer security policies, procedures, and settings) is a collection of documents issued by the US government about computer security. Every standard has some similarities and differences, and it can use them together to improve information protection in the public sector throughout an information security implementation. The advantages of the standards are multiplied when they are combined, resulting in a beneficial output.

**PCI DSS:** The PCI Security Standards Council created the PCI DSS as a collection of guidelines to enhance the security of payment card data. A data security standard for businesses that work with the branded cards of major credit card firms is the Payment Card Industry Data Security Standard (PCI DSS). The PCI Standard, which is required by the card brands, is administered by the Payment Card Industry Security Standards Council. To combat credit card fraud, the standard was established to tighten safeguards surrounding cardholder data. For data security and technological protection of payment systems, this framework contains highly specific and detailed standards, tools, measurements, and other resources. Any business that accepts credit card payments or conducts other forms of online transactions must adhere to these guidelines. The intentions were to provide card issuers with an extra layer of security by requiring merchants to follow minimum security standards while storing, processing, and transmitting cardholder data. The united work of the major credit card associations resulted in the publication of PCI DSS version 1.0 in December 2004 to address interoperability issues among current standards. The PCI DSS has been introduced and is being followed all around the world. Data related to credit card systems are also valuable and misuse of such data can result in financial crisis of the

customer. Thus, such security measures are important in systems including cards for payments.

**ITIL® & ISO 20000:** [ITIL](#), The UK Office of Government Commerce published IT Infrastructure Library, which was previously known as IT Infrastructure Library (OGC). The IT Infrastructure Library (ITIL) is an IT Governance framework that helps firms manage IT services more effectively. ITIL is a worldwide recognized set of best practice guidelines for IT service management in enterprises, and it is currently largely regarded as the most widely acknowledged model for IT service management in all types of organizations around the world (ItSMF, 2011). It is, without a question, the most extensively adopted approach for IT service management worldwide. It is a framework for defining, planning, providing, and supporting IT services to the business side of the organization. Although ITIL includes components of information security and service continuity (i.e., business continuity) management, it is not the primary focus of ITIL. Individual ITIL certification is quite common, but corporations cannot be certified against this framework. Organizations can get certified against the ISO/IEC 20000-1, a global standard based on ITIL. There are five phases in the ITIL V3 framework:

1. Service Strategy,
2. Service Design,
3. Service Transition,
4. Service Operation,
5. Continual Service Improvement (ItSMF, 2011).

**ISO 22301 and BS 25999-2:** [ISO 22301](#) is an international standard published by ISO that focuses on developing a Business Continuity Management System. It was published recently, but it is a new and improved version of British Standard [BS 25999-2](#), which had already established itself as a leading business continuity standard around the world. ISO 22301:2019 (International Organization for Standardization), The International Organization for Standardization published a management system standard that outlines standards for security and resilience-based business continuity management systems for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and constantly adding new a documented management system to prevent, minimize the likelihood of, prepare for,

respond to, and recover from disruptive situations. Regardless of the shape, size, or nature of the organization, it is designed to be relevant to all of them or portions of them. Organizations that implement an ISO 22301-based business continuity management system (BCMS) can go through a formal evaluation process and achieve recognized certification against the standard. Internal and external stakeholders can see that the organization follows best practices in business continuity management thanks to a BCMS accreditation. ISO 22301 is entirely compatible with ISO 27001, and the two standards can be implemented together quite quickly, resulting in a solid framework for information security and business continuity.

**NFPA 1600:** The National Fire Protection Association of the United States ([NFPA 1600](#)) is a standard that focuses on catastrophe and emergency management, as well as business continuity. It is extremely popular in the United States, and the National Commission on Terrorist Attacks Upon the United States has designated it as the National Preparedness Standard. It has been adopted as a voluntary consensus standard for emergency preparedness by the US Department of Homeland Security. It should be familiarized by everyone engaged in emergency management or business continuity. NFPA 1600 has considered the gold standard in emergency management since its inception. It's a common standard that emergency management and business continuity professionals may use to plan for and protect their people, property, and businesses. NFPA 1600 is endorsed by FEMA, the International Association of Emergency Managers (IAEM), and the National Emergency Managers Association (NEMA). In fact, these groups collaborate with the NFPA on the standard's development. The standard includes the core aspects required for effective disaster management and business continuity and is widely utilized by companies of all sizes and from all industries in the United States and around the world. It covers program planning, implementation, execution, and training, among other things. In comparison to previous editions, the 2019 version has a larger emphasis on crisis management. The most recent version emphasizes the need of maintaining crisis communication skills, which includes implementing a viable emergency communication system. When calamity occurs, businesses must be able to communicate with both internal and external audiences. Compared to ISO 22301, it is more detailed in the area of crisis management.

### **The General Data Protection Regulation (GDPR)**

The Regulation supersedes the Data Protection Directive 95/46/EC and aims to standardize data privacy legislation across Europe for the protection of individuals with regard to the processing of personal data and the free movement of such data. The General Data Protection Rule (EU) 2016/679 (GDPR) is a European Union (EU) and European Economic Area (EEA) regulation on data protection and privacy (EEA). The GDPR is an important part of EU privacy and human rights law, particularly Article 8(1) of the European Union's Charter of Fundamental Rights. It also handles personal data transfers outside of the EU and EEA. The GDPR's main goal is to give people more control and rights over their personal data while also making the regulatory environment for multinational business easier to navigate. [1] If either party (the "Receiving Party"), its agents, contractors, or employees are given access to personal data held by the other party for any reason, or if the Receiving Party, its agents, contractors, or employees are supplied with or otherwise provided personal data by the other party for any reason, the Receiving Party, its agents, contractors, or employees must comply:

1. Use and/or hold such personal data solely for the purposes and in the manner directed by the other party, and shall not edit, amend, or delete such personal data in any other way.
2. In all respects, comply with the Regulation and local applicable law, and do not do or authorize anything that would risk or violate the terms of the other party's notice under the Regulation or local applicable law.
3. Indemnify the other party against all liability, damages, fees, claims, and expenses incurred as a result of any default under this clause or any breach of the Regulation or local relevant law attributable to the other party.

#### **2.2.4 Socio-Technical Perspectives**

The purpose of IS research was to learn more about the nature of innovation as a result of the development, implementation, or design of an information system. As a result, there has been a lot of debate from the beginning about whether IS development processes can be considered instead of new technological systems, new socio-technical arrangements for processing information in an organizational setting should be used. Even though no precise definition of the term "information system" has ever been agreed upon, there is an unspoken understanding in the IS community

that it refers to information content, social context, and technologies. Recent ISMS specialists argue that Socio-technical system require bridging between hardware, software, employee and community characteristics. A relationship and combination of social and technological perspectives. Among them the human factors come out as a key element for effective ISMS that have to be secured by the managing body of the organization. People are the most crucial part of information security management. Within organizations, employees have a two-way effect. Employees, on the one hand, can play a negative role by stealing information with malice aforethought and violating access regulations, posing a significant threat to commercial enterprises. Whereas employee compliance with security policies, awareness, and training will have a significant benefit on information security. As a result, a more thorough examination of human aspects is required in order to eliminate human deficiencies and increase efficiencies for improved information security management. Management can play a critical role in information security management by monitoring, managing, and redirecting employee behavior, as human resources management is an element of firm management.

Dhillon and Backhouse (2001) suggested socio-technical aspect of Information Security in such a way that determines the need to realize the interaction between technological assembly and social outline in order to confirm appropriate security. Their intention was to figure out the political, common, cultural and ethical aspect of Information Security system. Their contemporary author Eloff (2003) claim that an organizational ISMS comprises a lot of issues such as strategies, policies, principles, guidelines, regulations, code of conduct, technology, culture, human behavior, law perspectives and many more. All this environmental phenomenon should be considered while critically examine the organizational Information system security. In addition, for efficient information security management, existing literature also promotes the combination of technical and managerial operations. Technical knowledge in information systems is just as vital as managerial professionalism since information systems contain both hardware and software. The function of management and managerial practices was noted earlier in the literature, and some management academics have advised that managerial and technical operations be integrated and aligned. The integration of these two factors, both technical and

administrative, along with the other factors will assure the effectiveness of information security.

A socio-technical outlook defines institution as a combination of social and procedural systems. Social in terms of maintaining the social terms here within the office premises and procedural in terms of following a continuous process throughout the month. In the perspective of the ISMS revealed 05 (five) social elements (i.e., institutional configuration, employees' consciousness on Information Security, awareness and training, societal fences, and practical hurdles) symbolize the social sub-system and the hazard handle mechanism characterizes the technical sub-system. Societal fences can be in terms of body language or attitude that suppresses one's confidence level and practical hurdles can be in terms of technological difficulties.

### **2.3 Organizational Culture**

Organizational culture refers to the ideas, presumptions, attitudes, and communication patterns that form the distinctive social and psychological environment of an organization. Various studies identified culture as an important factor manipulating employs' performance, embracing of IT, process of integration of IT systems, ISMS, knowledge transmission and change management. Every individual may belong from a different culture; therefore, one might face difficulty in embracing the information technology terms or adapting the knowledge of ISMS and its importance in terms of data security. Raman and Wei (1992) added, culture has considerable influence on exactly by what means Information Security systems were observed, used, accepted and practiced.

A society's values, customs, and ways of life reflect its culture. People look to culture to reflect their attitudes, routines, and beliefs as well as to aid in the spread of technology. Our civilizations' most important facets—language, art, mobility, education, and religion—are all touched by technology. The culture of a community acts as a standard for understanding, interpreting, and assessing technology. Since technology has an impact on every area of culture, it dictates how culture evolves. Technology must be in tune with the social and cultural circumstances of the community in order to occupy the larger cultural dimension; otherwise, there would be a conflict between the advancement of technology and the preservation of cultural



values. People can express themselves freely in a technical world that is beyond their understanding with a reasonable equilibrium.

Hofstede (2001) explained culture as shared indoctrination of the mind which differentiates followers from one human group to another; collaborative and cumulative of shared features which affect group's reaction to its atmosphere. A single technological concept can be adapted at different levels from one human group to another because of the difference in perspective of the culture.

### 2.3.1 Organizational Culture (Bangladesh e-government initiative)

An organization's culture is typically described by a set of customs, beliefs, attitudes, and behaviors that are shared by most of its members. According to Schein (2004), this pattern of fundamental assumptions is the basic tenets that a particular group has created, discovered, or adopted as a means of resolving issues related to external adaptation and internal integration, and which have proven effective enough to be taught to new members as the proper framework for perceiving, considering, and feeling about these issues.

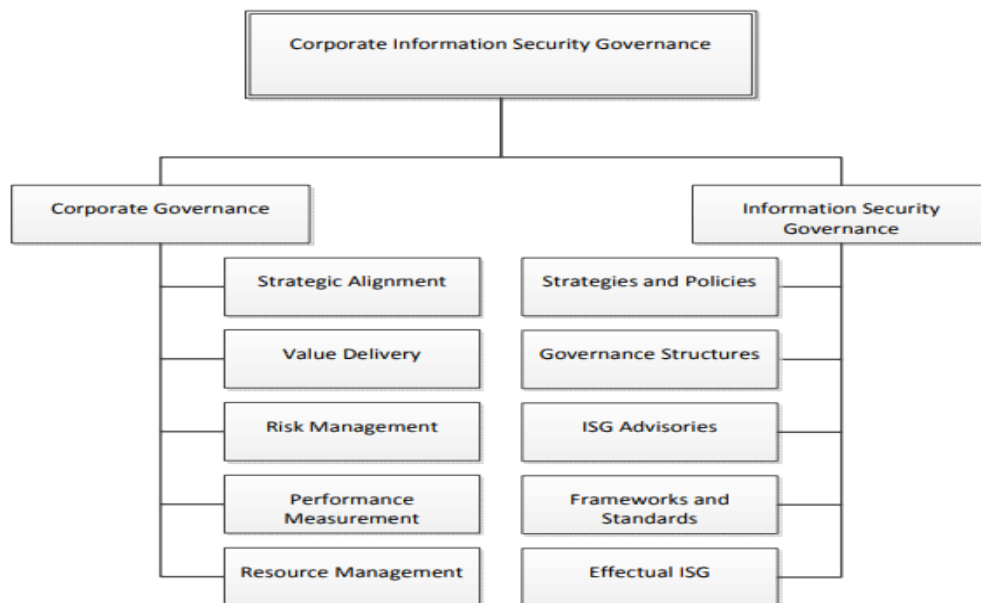


Figure 2. Corporate ISG literature review organization.

Electronic government, often known as e-Government, is a difficult concept to describe. E-government is still a developing field of knowledge, making it difficult to define precisely. "e-Government refers to government agencies' use of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that

have the power to revolutionize relations with citizens, businesses, and other branches of government," according to infoDev/World Bank (2009). "The use of ICTs, particularly the Internet, as a tool to accomplish better government," according to another definition of e-Government. Therefore, in all aspects, it is stated that e-government involves the activities in terms of technology, as a result the employees must acquire technical skills and adapt themselves to the technical environment. Here, culture plays an important role, according to and depending on the culture, the practice, adaptation, and rate of usage of employees may vary. One must not be hundred percent comfortable in terms of using technology where there lies a cultural gap. In addition, the workspace culture and environment also as an effect on the performance of the employees.

### **2.3.2 Relationship between ISMS and Organizational Culture**

Likewise, any other group establishment, government organizations have its own vision, mission, goals, values, prospects, and attitudes that convert into values (Hu, Cooke, Dinev & Hart 2012). First and foremost, the company must decide what sort of company it wants to become in order to build and cultivate an efficient workplace culture. In Bangladesh, government agencies are state-controlled institutions that act autonomously to carry out the government's policies. Government Ministries are policy-making entities with the authority to manage agencies through policy decisions. Some of the government's work is done through state enterprises or limited liability companies. An institution's setting symbolizes entire environments adjoining and touching administrative events (Davis, 2008). Maximum enterprises run in such an atmosphere that is influenced by alleged sponsor beliefs along with the office's aims, expectations and ethics (Hu et al., 2012; Davis, 2008). Public and institutional principles and philosophy, appropriate rules, guidelines and strategies, along with business performances, affect company staffs (Hu et al., 2012; Davis, 2008).

Organizational administrators, who control situation, should have effort to uphold the office principles. They try to regulate outside and inside factors influencing actions loyal to office vision & mission achievement (Davis, 2008; Steiger, Hammou, & Galib, 2014). Objectives are set in such a way to enhance product outcome, maintain social facts and etc. Executives normally want control basis which permits legislative arrangement, careful allocation of resources, adaptive threat calculations, standard

value delivery and exact quantities of employee performance with a view to fix security issues (Mohare & Lanjewar, 2012; Davis, 2008).

## **2.4 Areas of Exploration**

Different publication suggests that by this time new risks and threats are active on the horizon and they have relentless effort to attack on Bank and financial institutions, Law enforcing agencies, significant service rendering offices, vital information domain etc. Bangladesh Government has formulated adequate strategies, policies, controls and implementation plans to look over to the issues. Moreover, it has also a number of Cyber threat analysis units which continuously monitoring and sending alarm notice, if found necessary for any particular institution. These units keep an eye on receiving, assessing, and responding to occurrences and actions involving computer security in Bangladesh. The cyber threat analysis units respond to the necessary organization with a warning about the threat that has been detected in their analysis. The organizations are said to take necessary measures regarding the threat such as disconnecting their system from the internet, identifying the virus containing resource etc. In several studies, it has been discussed that an early detection plays a very important role in quick recovery or less damage. The following study tries to find out evolving key threats and their consequent impacts on the organizations. Apart from this, there is also an intention to explore how organization's culture shape employees' attitude to face the security challenges with a view to protect sensitive information assets. Overall, discussing the organizations before and after consequences, pros, and cons of cyber-attacks.

## **2.5 Framework for Improving Critical Public Infrastructure Cybersecurity**

Now a days, the Government is dependent on the reliable functioning of its critical ICT infrastructure of various public enterprise as due to digitalization several activities are performed via digital system. Therefore, the data relies on and or is collected via the application program. As Bangladesh is evolving as a nation, the concept of Digital Bangladesh had led through several improvements in different sectors of the country. These all have been achieved under the proper government guidance that has led to appropriate resource usage, building good collaboration with other countries, attempting to build its own resources, the talent hunts and many more. Bangladesh is one of the fastest growing or developing country over the world.

Bangladesh recently launched The Bangabandhu Satellite-1 (Bangabandhu-1) as the country's first geostationary communications and broadcasting satellite. Furthermore, continuous government projects have concentrated disaster preparedness and recovery systems with amazing results. Although Bangladesh is vulnerable to calamities, the country has a proven track record of increasing human security and saving lives.

Moving on to information security risks, the rising complexity and interconnection of key infrastructure systems has been abused, putting citizen security, the economy, and public safety at risk. Cybersecurity risk affects a government's bottom line in the same way that financial and reputational concerns do. As a result, it is past time for Bangladesh's government to examine such situations and request that the necessary actions be taken. Such research studies will help government to highlight the significant points that must be enhanced to improve the overall information security management system. To strengthen the resilience of this public infrastructure government can built its own framework that works to solve and secure the organizations important data. The framework can be based on public organizations only as they are reported to serve and has a similar objective to obtain.

**Guideline for Information Security Policy, 2014:** While implementing e-Government, the Guideline emphasized the importance of safeguarding the safety of data that government entities have processed, stored, and digitized. The document attempts to assist government agencies in developing unique rules that are most relevant to their security demands by highlighting recent cyberattacks. The policy also lays out a strategy for information security as well as risk, threat, and vulnerability management.

**Bangladesh's National Cyber Security Strategy for 2014:** The National Security Strategy is addressed in the Strategy. This statement intends to provide a coherent vision for 2021 that keeps Bangladesh secure and prosperous by coordinating government, corporate sector, citizen, and international cyberspace security initiatives. Roles and responsibilities are well defined in this strategy. Recognizing the common nature of cyber weaknesses, this Strategy calls for a public-private partnership to combat cyber-attacks in the banking, utilities, and telecommunications sectors.

**Guidelines on ICT Security for Banks and NBFIs:** A "ICT Security Policy" that complies with this ICT Security Guideline and has been authorized by the board is essential for every bank and non-bank financial institution (NBFI). The policy includes apps, data and network, computers and peripherals, and other specialized ICT resources. A bank's information technology system's availability, reliability, and integrity are important to its service delivery. Each bank and non-bank financial institution (NBFI) is required to implement the necessary safeguards to protect its information systems as a result. A continuous awareness and training program for all levels of employees and stakeholders must be established by senior management at the bank or NBFI to demonstrate their dedication to ICT security. The policy needs to be updated frequently to reflect changes in the ICT environment, both inside the Bank or NBFI and throughout the sector. For better and impartial management of security events, policy documentation, inherent ICT risks, risk treatments, and other pertinent tasks, the bank or NBFI shall hire ICT security professionals to work in a distinct ICT security department, unit, or cell. An approved compliance plan must be submitted to Bangladesh Bank in the event of noncompliance problems. The exception must be granted just during a certain timeframe.

The document "Framework for Improving Critical Infrastructure Cybersecurity," published by the National Institute of Standards and Technology (NIST) on February 12, 2014, is known as the Cybersecurity Framework (CSF). It is one of the long-term safeguards for our cyber environment against national security threats, hazards, and challenges. The National Security Strategy is addressed in the Strategy. By coordinating government, corporate sector, citizen, and international cyberspace defense initiatives, the goal of this document was to develop a coherent vision for 2021 that keeps Bangladesh secure and prosperous. This National Cybersecurity Strategy lays out a framework for planning and prioritizing activities to control cyberspace and critical information infrastructure vulnerabilities. This Strategy greatly enhances the profile of cybersecurity inside our governments and sets defined duties and responsibilities in order to achieve the aforementioned goals. Because cyber vulnerabilities are shared, this Strategy also calls for a public-private cooperation to address the potential susceptibility of private sector-owned vital infrastructure in the banking, utilities, and telecommunications sectors to cyber-attacks. The framework is broken down into three sections:

1. Core: divided into five functions (Identify, Protect, Detect, Respond, Recover), 22 categories, and 98 subcategories, with thorough approaches to areas of cyber security.

Identify:

- Establishing the foundation of an Asset Management program by locating the company's hardware and software assets.
- Identifying the business environment in which the company operates, including its involvement in the supply chain and its position in the critical infrastructure sector.
- Identifying cybersecurity rules in place inside the organization in order to specify the Governance program and the governing laws and regulations for the organization's cybersecurity capabilities
- As a foundation for the organizations, asset weaknesses, external and internal organizational resource threats, and risk mitigation strategies are identified
- Establishing risk tolerances and identifying a risk management strategy for the company
- Developing a Supply Chain Risk Management strategy that includes priorities, limitations, assumptions and risk tolerances to guide decision-making in supply chain risk management

Protect:

- Physical and remote access safeguards for access control and identity management throughout the organization.
- Providing awareness and training to employees inside the organization, including role-based and privileged user training
- To safeguard the confidentiality, integrity, and availability of information, Data Security protection should be established in accordance with the organization's risk strategy.
- Maintaining and managing the security of information systems and assets by implementing information protection processes and procedures

- Maintenance, including remote maintenance, operations are used to protect organizational resources.
- Managing Protective Technology to ensure that systems and assets are secure and resilient in accordance with organizational policies, procedures, and agreements.

Detect:

- Ascertaining the detection of anomalies and events, as well as their potential impact
- Continuous Security Implementation Monitoring tools to keep an eye on cybersecurity incidents and evaluate the effectiveness of preventative measures, like network and physical activity
- Detection Processes must be maintained in order to provide knowledge of unusual events.

Respond:

- Assuring Reaction During and after an occurrence, the planning process is carried out.
- Managing communications with stakeholders, law enforcement, and external stakeholders during and after an event, if needed
- Analysis is done to make sure that reaction and recovery steps, like conducting a forensic investigation and determining an incident's impacts, are efficient.
- Mitigation operations are carried out to avoid the spread of an occurrence and to bring it to a close.
- Improvements are implemented by taking into account lessons learnt from current and previous detection/response actions.

Recover:

- Assuring that the organization's recovery plan is in place. Processes and procedures for restoring systems and/or assets that have been impacted by cybersecurity incidents are being developed.
- Improvements based on lessons learned and reviews of existing tactics are being implemented.
- During and after the recovery from a cybersecurity event, internal and external communications are coordinated.

2. Implementation Tiers: A corporation can use these four categories—partial, informed, repeatable, and adaptive—to describe its perceptions of cyber security risk and the level of sophistication of its management strategy to both it and its partners.

- **Partial:** This tier is for companies who do not have any security procedures in place. Tier 1 companies are regarded as having little or no cyber maturity. Companies in this class are notorious for not properly prioritizing cybersecurity settings. At this level, companies should try to understand and adequately address cybersecurity concerns.
- **Informed:** This grade is for companies who understand hazards and are presently addressing some compliance obligations but aren't addressing all security problems or policies across the board. Businesses in Tier 2 are often aware of some of their cybersecurity concerns, but they may not be addressing them rapidly enough.
- **Repeatable:** Tier 3 companies have risk management and cybersecurity best practices that have been endorsed by the CEO. This group of companies is more prepared to deal with cybersecurity threats, hazards, and vulnerabilities in their environment. Tier 3 companies spend more time engaging with other companies in their field and evaluating themselves against their peers to guarantee best practice alignment.
- **Adaptive:** Tier 4 companies will employ advanced adaptive cybersecurity practices. Adaptive security is a cybersecurity method that monitors behaviors or events in order to prevent against or react to attacks before they occur. The adaptive tier enables firms to continuously analyze risk



and automatically apply proportional enforcement based on prior experiences and current industry best practices.

3. Profile: a list of outcomes from which a company can select based on its business needs and individual risk assessments (Current Profile) as a way to promote prioritizing and monitoring of progress toward a desired risk level (Target Profile).

The broad category of technology supports the performance of services by information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT), SCADA. This reliance on technology, communication, and interconnection has changed and increased operational risk while also widening potential vulnerabilities.

Following Framework has been suggested by the NIST to protect critical cybersecurity infrastructure:

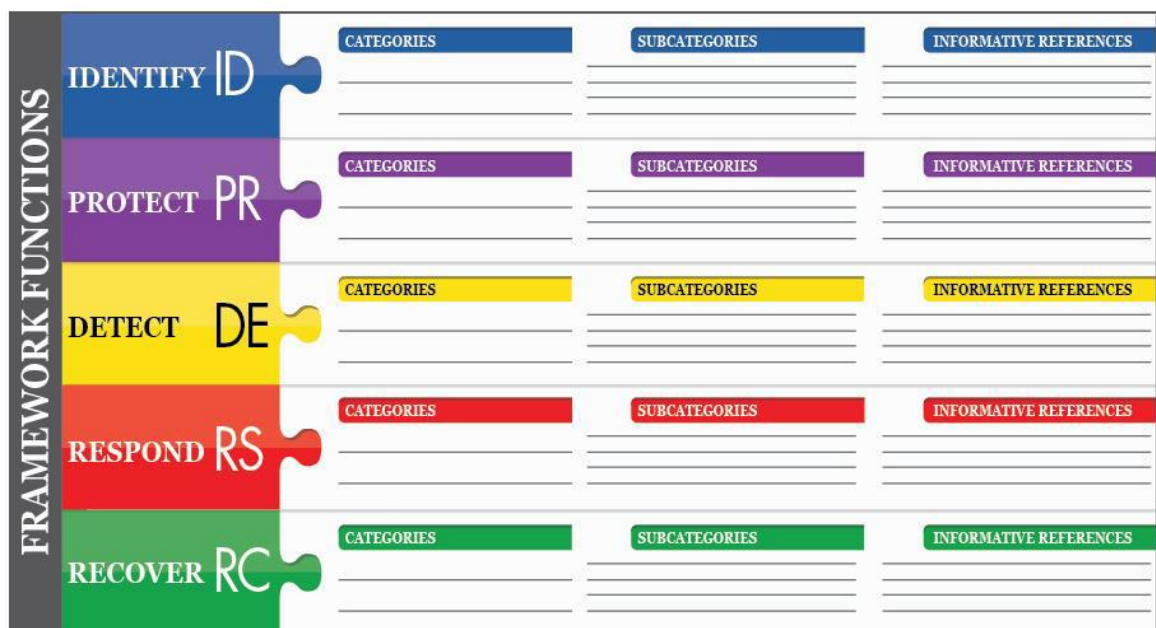


Fig 2.2: NIST-800 Framework to protect critical cybersecurity infrastructure (Source - <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>)

- **Identify** – Develop organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. For the Framework to be used effectively, the tasks listed under the Identify Function are crucial. By comprehending the business environment, the resources supporting critical

functions, and the associated cybersecurity threats, a company may concentrate and prioritize its actions in accordance with its risk management strategy and business needs. Examples of result categories under this function are asset management, business environment, governance, risk assessment, and risk management strategy.

- **Protect** – To assure the delivery of important services, develop and execute suitable measures. The Protect Function aids in limiting or containing the scope of a possible cybersecurity incident. Identity management and access control, awareness and training, data security, information protection policies and procedures, maintenance, and protective technology are a few examples of outcome categories within this function.
- **Detect** – To detect the existence of a cybersecurity event, develop and perform relevant activities. The Detect Function enables the detection of cybersecurity events in real time. Anomalies and Events, Security Continuous Monitoring, and Detection Processes are examples of outcome categories within this function.
- **Respond** – Create and put into action appropriate responses to an identified cybersecurity occurrence. The Respond Function assists in limiting the effects of a potential cybersecurity problem. Response planning, communications, analysis, mitigation, and improvements are a few examples of result categories within this function.
- **Recover** – Create and put into practice appropriate measures to sustain resilience plans and to repair any capabilities or services that have been damaged as a result of a cyberattack. To minimize the impact of a cybersecurity incident, the Recover Function facilitates a quick return to normal operations. Example of a successful outcome Recovery Planning, Improvements, and Communications are all categories within this function.

### **Implementation of Security Operation Center (SOC) for public enterprise**

The COVID-19 pandemic period has provided cyber criminals with a wide range of opportunities due to a worldwide lockdown during which all offices were closed and critical security precautions were not taken. Such events are of significant interest to cyber criminals because it is relatively easy to gain access to any system during this

time due to a lack of maintenance, upgrades, and usage. Cyber criminals are always developing new tactics in their attacks, making it harder for older frameworks to keep up. Their efforts to hack computer systems have been steadily rising. As cyber criminals become more skilled in their infiltration techniques, the existing level of security processes may offer a greater threat to organizations. To protect government enterprise from rising cyber threat today need a balanced security solution that is ability to offer both preemptive defense and flexible expansion. The government is spending billion dollars annually on cybersecurity tools, processes, and people to protect government enterprise from cyber threat but spend more does not always mean fruitful outcome. As the government enterprises consists of valuable data and any misleading of such data can have very negative effect on the overall economy. An effective Threat-centric SOC is needed to overcome is which is consists of high professional expertise and skills with new technology equipment, top security intelligence data, and advanced analytics with help of artificial intelligence (AI) and Machine Learning (ML) to detect and investigate threats with great efficiency, accuracy, and focus. Threats can be identified prior and informed to the respective organization to take necessary measures. The process keeps constantly working and detects threat patterns, reports, and executes necessary actions. A threat-centric SOC proactively hunts for malicious threats on cyber infrastructure of the organization. A typical SOC architecture is showing below

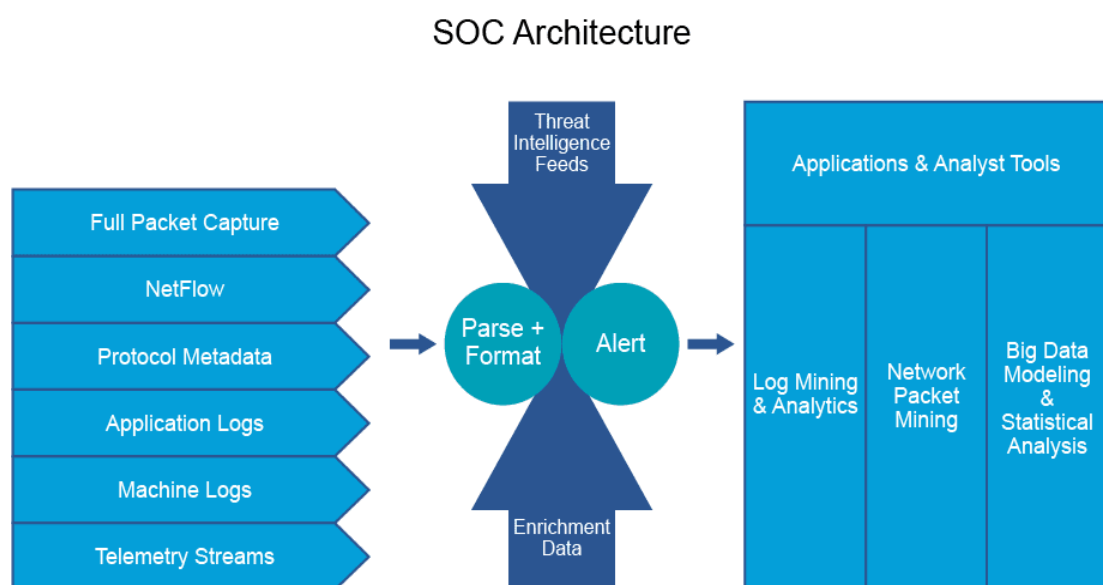


Figure 2.3 SOC Architecture  
 (Source- <https://whilenetworking.com/2018/08/06/security-operations-center-its-types/>)

**Full packet capture:** Packets are recorded and analyzed to assist in the diagnosis and resolution of network issues such as: Detecting security risks, troubleshooting a network's unfavorable behavior, detecting network bottlenecks, Detecting data and packet loss and Network analysis for forensic purposes. It is possible to capture entire packets or chunks of a packet. A complete packet consists of two parts: a payload and a header. The payload contains the packet's actual contents, whereas the header contains metadata such as the packet's source and destination addresses.

**Protocol Metadata:** The metadata of a network is a record of all communications that take place within it. It keeps track of what, when, where, and with whom network communications occur. Network captures are high-resolution data streams that include connection and payload information. Metadata for a particular protocol is Protocol Metadata.

**Application logs:** An application log is a collection of events recorded by software. There are mistakes, informative events, and cautions all around.

**Machine logs:** Appliances, software, machines, and networking devices all produce machine logs (switches, routers, firewalls, etc.) Every event is systematically written to a log file including all of the logs, along with its details.

**Telemetry Streams:** Streaming telemetry is a push-based approach that eliminates polling's inefficiencies. Without the need for polling, the essential data is transmitted automatically and constantly from network devices to management systems.

**Log mining and Analytics:** Log Mining technique for analyzing logs that employs Data Mining. The quality of log data analysis has improved since the advent of the Data Mining technique for log analysis.

**Network Packet Mining:** Network data mining and statistical analysis are used to evaluate traffic loads, analyze user behavior patterns, and forecast future network traffic.

**Big data modelling and statistical analysis:** Modelling the big data obtained from the several process executions and producing a statistical analysis from the results obtained.

## **Endorsements for effective information security in the public sector**

If one wants information security to be effective, a number of tasks must be carried out continuously. Resources must be invested in advance to stop such assaults and lessen the loss because cyberattacks cause significant resource and asset loss. These spend a lot of time and money on technology, personnel, and processes, and after the implementation is complete, they discard all the rules, guidelines, and tools since they are no longer relevant and useful. The following activities should be prioritized in order to maintain and enhance your system.

**Monitoring:** People who are responsible for safeguards will have to track how they are performing. Such as management, management is responsible for non-technical components of information security such as security policy formulation, awareness training, hardware and software acquisition, internal control, and data processing decisions. Management would struggle to manage information security without technical assistance from IT and security professionals. On the other hand, without management support and involvement, IT professionals will be unable to protect information resources. The continuous monitoring of the management helps to early detect and identify faults in systems as a result, information resources are kept well protected from threat. Continuous monitoring also enables to report system bugs and can enhance overall system performance.

**Measurement:** In contrast to monitoring, measurement is carried out on a regular basis (such as quarterly or yearly), with the aim of determining if goals are being reached. Measurements of the policies obtained to ensure whether they are working on full phase or not. Easy to report the result and take necessary steps to solve. Measurement will also be performed by organization officials, and it should be considered as a prime responsibility to save the institution from cyber-attacks.

**Listening to suggestions:** All interested parties (workers, partners, clients, government agencies, and so on) are likely to be aware of where organizational security is deficient. People must ensure that communication lines remain open, and that all information is sent to the appropriate individuals within your organization. The organization's culture and environment must be set up in such a way to encourage communication among staffs, this will also lead to rise in productivity. It is considered that the employees will acquire cyber security management awareness

training prior being involved in it so that they can relate with the terms and perform better. Employee skills and knowledge are very important in all its perspective. Once they are aware of the consequences, then they can easily put on some efforts or suggestions for the betterment.

**Internal audit:** Conduct audits of vendors and partners who have access to sensitive data and systems. Third-party (contractors, vendors, and partners) control should be a significant priority area for organizations' essential information. Organizations must ensure that third-party information security is adequate and appropriate. Data can be mismatched or manipulated from the third-party ends as well. Finally, an internal audit could be the most important factor in improving the security of your data, ensuring that it is kept safe.

**Top management review:** Members of upper management should set aside some time for cybersecurity every now and then (for example, quarterly). All detected threat instances, their reports, and analysis results should be clearly known to top management officials. Top executives should make important decisions such as changing cybersecurity objectives, allocating resources, making organizational changes, removing implementation roadblocks, organizing workshops and trainings for employees to improve their skills and knowledge in cyber security management, and so on.

**Continuous improvement:** Continuous improvement is a continuous process of improving products, services, or processes. These attempts can aim towards "gradual" development over time or "one-time" breakthroughs. All the above activities will result in a To-Do list that must be completed. Corrective and preventative actions are a notion in ISO standards that describes a practical technique of tackling these lists in a systematic manner. They must be listed in a straightforward manner, with clear timelines and responsibilities, and each one must be checked once implemented to ensure that the problem has been solved. The process has to be continuous as at any time, there might be any encounter of threat.

**Security Awareness and Training:** As technology advances, organizational institution must ensure that all relevant staff receive appropriate training, education, changes, and understanding of ICT security operations that are relatable to their work function. A minimal level of Business Foundation Training for ICT staff must also be

provided organizations. All employees must receive security awareness training/workshop from the organizations. Considering any new financial services or technical advancements, the organization must provide suitable training/awareness facilities for the IS Audit team.

**Insurance or Risk Coverage Fund:** In order to limit the costs of loss and/or damage to ICT assets, sufficient insurance coverage or a maintaining risk coverage fund is necessary. If relevant, the risk coverage fund must be correctly kept in the organization's accounting system. If the risk coverage fund is maintained, there will be a clear policy to use it as necessary.

## 2.6 Policy Implementation

The primary goal of the ICT policy is to encourage the multipurpose use of ICT to ensure government accountability and transparency, the development of human resources, the provision of public services with the involvement of the public and private sectors, and the achievement of national development goals by 2021 and 2041.

The following represents some of the ICT Policies in Bangladesh:

### **Implementation of ICT in Healthcare:**

- Extending geographic access: By displacing a conventional office visit, the goal is to overcome the gap between the patient and the doctor. It covers what is typically referred to as telemedicine (e.g., a hotline number, a video conference with patients in remote locations, or instant messaging with a doctor for medical advice).
- Facilitating patient communication: The goal is to make it easier for patients and healthcare professionals to communicate outside of normal office visits. Subcategories consist of:
  - a) general health education
  - b) encouraging patient compliance
  - c) enabling emergency care
  - d) protecting patient privacy.

- Enhancing diagnosis and treatment: By providing real-time support for clinical decision-making and diagnosis, the goal is to enable a health professional to perform clinically better during training or in the field.
- Improving data management aims to enhance data gathering, organization, and analysis. It can facilitate remote data collecting, speed up data transmission, and improve data quality (e.g., Using personal digital assistants to gather data electronically on specific diseases or the health of children in specific regions, for instance; electronic record systems). Subcategories consist of
  - a) data collection
  - b) data organization/analysis
- Financial transaction streamlining: The goal is to speed up financial transactions by making it simpler for patients to pay for their care and for doctors to collect the payment (e.g., mobile insurance premium payments, vouchers over the phone).
- Preventing fraud and abuse by mitigating fraud and abuse (e.g., Using biometric information to establish that a health practitioner has truly visited a patient, using messages and pin numbers to identify fake medications). Subcategories include:
  - a) verifying a medical product
  - b) verifying patient identity
  - c) verifying financial transactions
  - d) Tracking human resources/operations.
- Other: These includes fewer common categories like overcoming language hurdles or utilizing the allure of technology to draw in more patients and attention.

### **ICT in business**

This component will deal with three broad issues of Digital Bangladesh namely

- i) ICT as an export-oriented sector
- ii) Market access
- iii) Business promotion to support Digital Bangladesh, and.



This component's main goal would be to use ICTs to support the access of underserved producers and companies to markets. This extends to the concern of utilizing ICTs to uphold a just and socially responsible market for all. The issue of ICT business promotion would be the second sub-component. The primary goal is to support the sector so that it can offer the services and technology required to keep the other three elements of Digital Bangladesh operating. To increase its capacity for ICT export and generate foreign money, the third sub-component entails promoting the ICT business sector.

### **ICT in Education**

To fully utilize ICT, the Bangladeshi government created the National ICT Policy in 2002. In 2009, the National ICT Policy was updated. All the elements of the National ICT Policy 2002 have been more explicitly incorporated into the National ICT Policy 2009. The following list includes some of the precise policy declarations pertaining to education:

- To address the short-term skills deficit in the ICT business, evaluate the abilities of experts in the field and fill any gaps with focused training programs.
- Encourage greater cooperation between the academic and business communities to better match curricula to industry demands.
- Build an ICT Center of Excellence with the required long-term financing to provide instruction and support for advanced ICT research.
- Improve education at all levels, putting a particular emphasis on English, Mathematics, and Science.
- Increase the use of ICT tools across the board, including in ECDP, mass literacy, and lifelong learning.

### **ICT in Disaster and Emergencies**

One of the hardest problems has historically been getting emergency services into rural Bangladesh and getting them there quickly. Emergency services were formerly solely accessible to the wealthy, but mobile services significantly improved access to

them. Additionally, it enables families to stay in touch with one another during natural catastrophes, maintain contact with aid workers, and gather knowledge that will enable them to quickly get support.

## **ICT in Government**

### Prime Minister's Office (PMO)

- There is now a National ICT Task Force, and the Honorable Prime Minister is its leader.
- The ICT Task Force is made up of representatives from many significant ministries, academics, NGOs, and the commercial sector involved in ICT.

### Ministry of Science and ICT

- Creating an ICT policy
- Making ICT-related laws
- Enabling computerization in government agencies and educational institutions

### Ministry of Post and Telecommunications

- Building and maintaining of telecommunication infrastructure

### Ministry of Education

- Curriculum for ICT education
- Computerization of schools

### Ministry of Law, Justice and Parliamentary Affairs

- Laws relating to ICT
- Department of Planning, Ministry of
- Administrative assistance to the National ICT Task Force
- Coordinates the Support to ICT Task Force (SICT) Program, which carries out the ICT Task Force's goals, especially in the area of e-Government.

### Bangladesh Telecommunication Regulatory Commission (BTRC)

- Regulation of telecommunications providers
- Licensing authority

### Bangladesh Computer Council (BCC)

- ICT training for residents and government employees
- Software company incubator
- Providing government organizations with ICT advisory help
- Providing ISPs with connectivity
- Standardizing ICT-related concerns, including keyboard
- ICT education curriculum

## CHAPTER III: THEORETICAL FRAMEWORK

### 3.1 Overview

Today's organizations across the world are significantly reliant on digital methods where Cyber system and Information security become the key strength of their day-to-day activities. Lots of theories are there to explain security compliance issues. Those theories have been used extensively in innumerable literatures with a view to describe and calculate information risk and vulnerabilities. To get a dense confirmation of prevailing theories on Information security, a methodical literature review has been performed in the previous chapter. Through a careful assessment of theories those have guidance on organizational information security, the research focuses on the following theories for the research.

### 3.2 Relevant Theories

Kerlinger (1979) defines theory as "a collection of interconnected variables, definitions, and propositions that gives a systematic picture of phenomena by establishing relationships among variables with the goal of understanding natural occurrences."

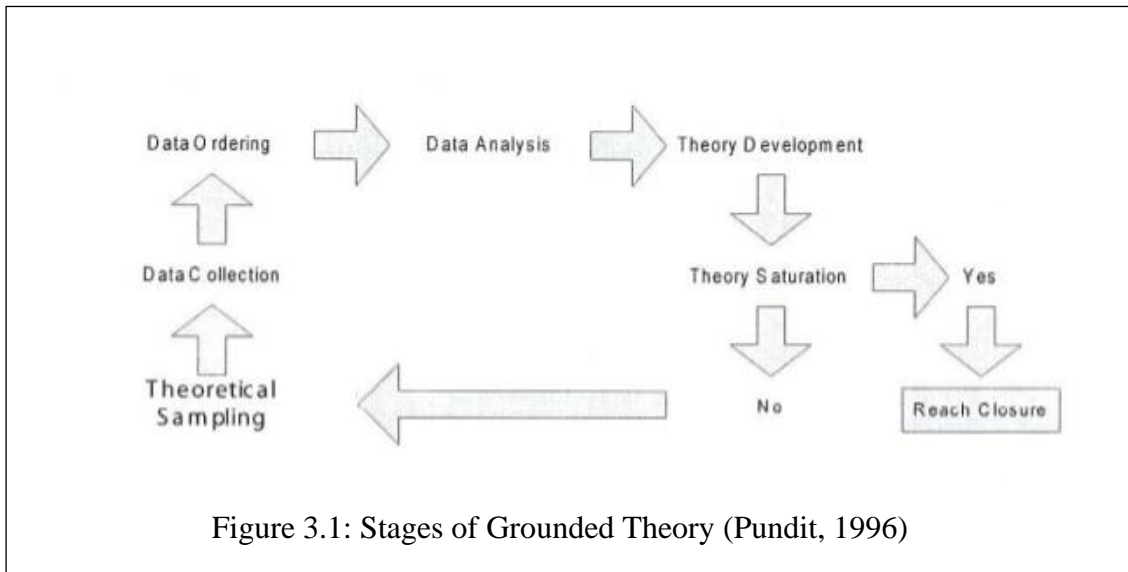
Cybercrime is a continuous and evolving challenge for both government and non-government organizations across the globe. According to Ousley (2013), State of cyber security capacity of any organization could be defined on five dimensions, those are- Information Security procedure and plan, Organizational security culture, Information Security learning, exercise and abilities, Law and governing framework, principles, organizations and know-hows.

In this research, it is going to find out how information Security incidences influence organizational prosperity. While do so, it believes that the following theories will guide it towards a new knowledge.

#### 3.2.1 Grounded Theory

*Grounded Theory* is called an organized and qualitative way to formulate concepts constructed on the collected data (Gupta and Raj, 2009). In his study, Knapp (2005) used this theoretical approach. He collected data through performing semi-structured

interview crafted with some open-ended questionnaires. The researcher systematically analyzed those data and successfully developed a theoretical model.



### 3.2.2 Socio-technical system theory

Schneberger & Wade (2008) argued that social and mechanical systems should consider collectively with a view to increase the efficiency of organizations. *Socio-Technical system* theory reveals that executive systems are comprised of socio-technical systems, which are self-governing and collaborative. While discussing Socio-Technical theory Chaula (2006) stated “examining culture, usability problems, internal security controls and security requirements by combining both technical and social aspects provide a more efficient perspective for modeling and developing information security system”.

### 3.2.3 Socio-psychological theory

Nowadays, organizations across the world are greatly reliant on digital arrangement. Information System as well as its safety and security become pillar of day-to-day actions and activities.

Sommestad et. al (2015) claimed that employees’ behavior shows an essential part for information security in organizations. Safa et. al 2016 pursued Social Bond Theory who defines social bonds “... between specific person and his group where the individual is obviously inclined towards offense but persons with stronger social ties are less attracted to indulge in any antisocial or deviant behavior”.

Ifinedo (2014) evaluates Social Cognitive theory as the simultaneous and dynamic interaction between common and personal variables where individuals are aggressively tangled and attain necessary consequences when they consider their actions are under their mechanism.

### **3.2.4 General deterrence theory**

Basically, *General Deterrence Theory* has been derived from Criminology discipline. It focuses on deterrents and approvals against a criminal act (Nagin, 1998).

According to the doctrine, preventive activities in an organization should have impact on the personnel and collective conduct and their intent about crime. Rajab & Eydgahi (2019) pronounce "... serious, rapid and certain penalties discourage employees from particular behaviors." Information Security researchers referred deterrence theory to envisage user behaviors those are either helpful or troublesome for Information System security and other security related variables.

### **3.2.5 Institutional theory**

Institutional theory enlightens the procedures and causes for institutional behavior and the consequence of organizational performance patterns within a broader, inter-agency perspective. It also argues that organizational entrepreneurship is a process by which agents change present institutions into authorized fresh practices to recognize highly valued benefits.

Paul DiMaggio (1988) emphasizes on entrepreneurs' tactics for building up logics in order to facilitate adjustment and for mobilizing capitals, and how new ideas become amalgamated into the institutional constraints on an organization. According to Tuffield (1975) Institutional (Organizational) theory explains what personnel in and around organizations think, feel and do.

### 3.3 Conceptual Framework for this Research

Ravitch & Riggan (2016) argue “A conceptual framework aids in first identifying and then clarifying the key elements of a study that are valued, known, and cared about, and then connecting them to the study's other components and external factors”.

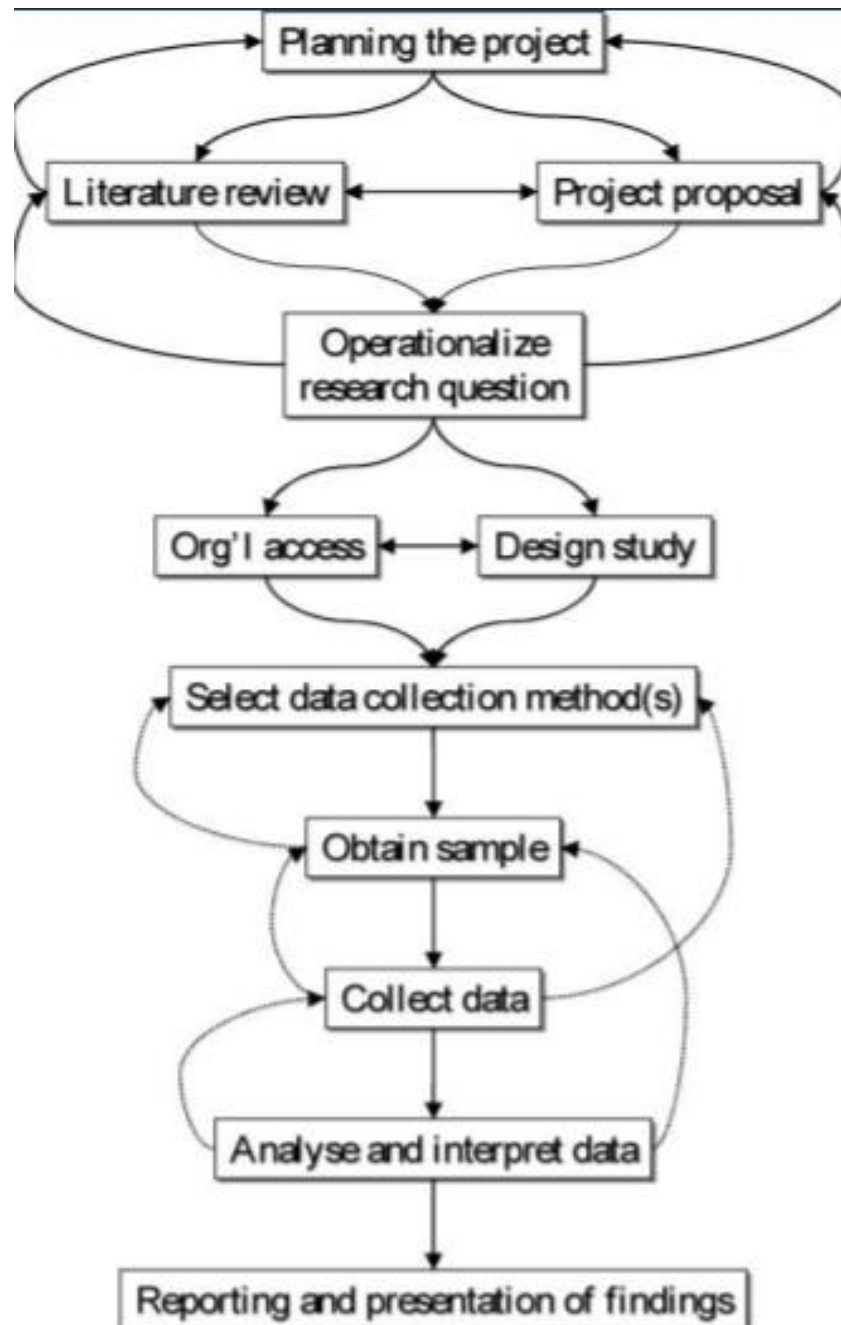


Figure 3.2 Conceptual Framework of the Study  
Source: Brewerton and Millward, 2014

### **3.4 Relevant values of the Institutional Culture**

This research has another intention to figure out whether there is any connection between information system and organization values. According to Nosworthy (2000), an organization's culture has a significant impact on organizational security since it can 'hinder change.' According to Borck (2000), "successful security must include the company culture as well as the latest technology.". Different research paper advocates that the research on security culture cannot be conducted in separation of broader organization culture. With this in mind, Detert et al(2000) .'s definition of eight "overarching, descriptive cultural characteristics" is adequate for identifying security principles across a wide range of businesses with varying levels of security. "The basis of truth and rationality, the nature of time and time horizon, motivation, stability versus change/innovation/personal growth, task/work/coworker orientation, isolation versus collaboration/cooperation, control/coordination or responsibility, and finally orientation and focus," according to the report.

### **3.5 Implication of Theories in Information Security Research**

The studied concepts in this paper have added an enhanced thoughtfulness about Information Security, obedience, behavior and therefore, able to outline actual safety procedures to inspire Information Security protocols. Forthcoming research could focus upon implication of those ideas in forecasting Information Security acquiescence performance improved.



## CHAPTER IV: RESEARCH METHODOLOGY

### 4.1 Overview

Generally, Research Methodology can be simplified as a process or strategy, or plan of action where particular methods used are supposed to bring out desired outcome. The purpose of this paper is to achieve an in depth understanding from the interpretation of incidental impact of escalating information threats on Critical Information Infrastructure of Government organization. So, the research has followed '*Qualitative Research Methodology*'. The goal of this research is to discover a theory that describes the phenomena of several Information threats through content analysis of primary and secondary data.

### 4.2 Justification of the Methodology

A suitable research design is vital element for piloting research because this element helps define research quality (Wahyuni, 2012). Qualitative research emphasizes socially constructed nature of reality, the association between the researcher and research phenomena, along with the situational checks that outline the investigation (Welford et al., 2012). Qualitative methodology has become progressively a widespread approach in the discipline of social science research. Primarily it is researcher's responsibility to scrutinize and make a choice about which research methodology, or blend of approaches should be followed research.

There are enormous studies that suggest qualitative methodology for doing research in Information Security. Here are some reasons in favor of qualitative methodology-

First, my research aimed to accomplish an in-depth understanding about the most pertinent information risks, threats and vulnerabilities usually takes place in Bangladesh Government Critical Information Infrastructure and how do they affect the organization. The main concentration of this study is to explore the incidental impact of several information threats in a public enterprise. Qualitative methodology is characterized as interpretative exploration as it pursues to advance understanding through comprehensive description towards theory building.

The second point is that, since Qualitative methodology is interpretive in nature, such study allows me to reveal the effectiveness of existing threat protection mechanism and some other unanticipated incidences.

Next, Qualitative research methodology is frequently associated to perform small scale study. It is very much related with the Covid-19 situation where large-scale investigation is literally challenging. Collection of data has been performed through Interview and KII (over telephone, zoom meeting and WhatsApp call), focus group discussion, participant's observation.

Finally, while doing Qualitative methodology, the researcher has the option to examine and observe how and why organizations accept and design their prevention and response information security management practices. Qualitative methodology permits the researcher to understand and get insights about people in their own terms, whereby deep and detail thoughts emerged through straight citation and careful explanation.

### **4.3 Sampling Procedure**

Sampling is a scientific method of reaching conclusions about a population without learning everything there is to know about that population (Rao, 2012). Given the resources available, such as money, time, and research design, as well as demographic characteristics, sampling is thought to be one of the best ways to collect data.

This research is about to explore information risks, threats and vulnerabilities which mostly focuses on the features and mechanisms of Information Security. It is in-depth in nature where mostly interview based methods have been adopted.

In the social and behavioral sciences, sampling processes are frequently classified into two categories: probability and purposive. A purposive sample is intended to select a limited number of instances that will provide the greatest information on a specific phenomenon, whereas a probability sample is intended to select many examples that are collectively representative of the population of interest (Hayat, 2013).

The sample size for this research activity was justified based on some definite empirical research. Srnka and Koeszegi (2007) suggest that qualitative methodology has been characterized by the procedure of small samples, often in between six (6) to thirty (30) respondents.

## **4.4 Source of Data Collection**

Direct interaction with individuals on a one-to-one or group basis is frequently required when collecting data using a qualitative approach. For the purpose of analyzing different facets of the research issues, multiple sources of data were utilized including various government agencies. As a result, the study relied on primary data gathered through interviews, observations, and informal discussions, as well as secondary data gathered from official records, newspapers, and prior studies, book publications, maps/images, journal articles, reports, and other materials. It should be noted that, while the data sources varied in their role and value throughout the study, they all worked together to complete the picture.

### **4.4.1 Government Organizations as Data Source**

This study relies on various government organizations as a major source of the data it incorporates to perform its analysis and to present the results and findings. Open data from government organizations plays a vital role in today's world. Administrative data is information gathered when providing government services. Such data are especially valuable to academics since they offer a wealth of information regarding populations. These massive data sets can then be analyzed to yield crucial insights that are valuable in a variety of ways. Digital storage expands the possibility for data utilization, while improved computer power makes data analysis and actionable insights easier. In both the public and private sectors, personal information is used to draw conclusions. Questions about how data is used, maintained, and who has rights to it are prompting government entities to reconsider the data they gather and what they do with it. The digital society in which we now live have both possible threats and advantages. Surveillance, loss of privacy, bias, and loss of reputation and autonomy are all risks. Advantages, on the other hand, include the utilization of data for analysis, which leads to new insights about effective services that encourage and support the flourishing of individuals and communities. The way data is used seem to have significant implications for specific groups of people or communities, as well as individuals. An examination of data, for instance, may inspire conclusions about any given service; for instance, a determination that a person or a specific group of people is unlikely to benefit from a particular service and should hence be ineligible for that facility. Indeed, data sharing projects may fail if public consequences such as these are not recognized, or the public is not informed about such.

Government regulations restrict how administrative data can be shared with academics. These restrictions preserve data, sometimes at the expense of study, by making data acquisition slow or impossible. Most types of data should not be stored in a single large database in a single location, nor are they controlled by a single entity. Rather, each organization handles its own data, such as a specific ministry or a department inside a larger organization. In most circumstances, a data steward or privacy officer is selected to accept or deny data access privileges. Every person might view privacy restrictions differently, or they may disagree on what to provide with the experts; it could delay on receiving the data and beginning their analysis. While privacy regulations or other regulations serve to set certain bounds for data usage, the data ecosystem is fast evolving as academia and government specialists demand better accessibility. There are no apparent answers to such concerns since they entail the evaluation of conflicting ideas, such as the need of safeguarding confidentiality versus the importance of conducting research for the general good. Various groups and people may evaluate the optimal balance individually. As a result, it is critical to involve the public in the development of standards and guidelines for data use.

Available government data is essential information that is both free and freely accessible to anyone, with no limits or constraints. Authorities are especially keen in encouraging this new method of connecting with their citizens. Many government agencies have begun to see the advantages of operating in a more open and transparent manner. Laws, policies, and procedures, as well as government performance, are all made available to the public through a single source. Here are a few insights that are observed during the data collection period of this study of how transparent democracy can result in a more productive and effective administration:

- The tendency to publicly accessible implies that members of the public can keep engaged, aware, and kept apprised with their local administration's day-to-day activities. Because this information is public, governments are held accountable for the outcomes they produce. Residents can see exactly what their government has accomplished and how much more has to be done. Failure to achieve certain results or accomplish a specific milestone or objective will be reported and scrutinized. In contrast, meeting or exceeding

targets will assist to build a stronger and more trusted relationship with local communities.

- The transparent nature of publicly accessible data exposes an aspect of an organization which is rather often kept under wraps. This level of sensitivity and openness is equivalent to revealing pieces of your personal life with another individual. An open and honest dialogue fosters a great deal of trust and respect, and the consequence is frequently a tighter and more dependent connection between the two individuals. Similarly, open government data contributes to the development of confidence and credibility among citizens. Residents can have peace of mind knowing that their local government is working hard to keep commitments and make decisions that are best for the community.
- When critical performance data is released into the public domain, its value has few limitations. Open data releases new commercial uses, reduces time-to-market for enterprises, and can provide the groundwork for future technical innovation and economic growth. Third parties who do not have the means to collect this data will be able to repurpose it and use the information to generate new applications and services. This type of information is also useful to academic, public-sector, and industry-based research communities. Open data greatly raises the value of information by allowing it to flow and be fully exploited.
- What better approach to enlighten the populace about the development and performance of the city than to have everything displayed in a simple and straightforward manner? By making the data widely available, open government data enables you to proactively respond to those often-asked queries. The public can participate and provide helpful comments at any point during the process because information can be made available as soon as it is obtained. A community can become more cohesive and empowered to influence the future by having access to useful data.
- The capacity to utilize both current information and historical data that has been accumulated over time is facilitated by the availability of consolidated information in a single, easily accessible location. All information will appear where and how it is expected to, and it will stay in that area for future use,

thanks to this method of data storage. The ability to spot trends and changes in the data over time is also made possible by this.

Data shared by the government organizations are very much important and crucial to do analysis on and to gain insights on various government initiatives and policies and their implementations. Thus, this study incorporates the data that are made publicly available by the four major government organizations of Bangladesh. In detailed approaches of data collection are elaborated in the following subsections.

#### **4.4.2 Primary Data**

##### **4.4.2.1 Interview**

In this research a semi structured interview with purposive sampling procedure have been carried out for primary data collection. The interview respondents were identified by their respective working head of organizations. Most of the interviewee was medium to highly responsible IT expert deployed in government domain. The participants comprised of both male and female employees. Statistics showed that most of the respondents had significant IT working experience in the Government sector and that their replies may be considered valuable for this study. With a view to cover a possible extensive area of population, some vital personnel from the academia and non-government sectors who are recognized as expert in cyber security arena were chosen to participate in the interview session.

A semi-structured interview with open-ended questions were carried out to gain a thorough grasp of the 04 (four) government entities' current standard security processes.

##### **4.4.2.2 Personal Observation**

Furthermore, observational data are utilized to describe organizational environments, activities, individuals, and the interpretations of what is observed from the perspective of the participants. Because it gives information of the context in which events occur, observation can lead to a deeper understanding than interviews alone because it allows the researcher to notice aspects that participants are unaware of or hesitant to discuss.

##### **4.4.2.3 Key Informant (KI) Interview**

A qualitative in-depth interview with persons who know what's going on with the research topic is known as a key informant interview. The goal of key informant

interviews is to gather information from a wide range of persons who have firsthand knowledge of the issue, such as community leaders, professionals, or residents. These domain specialists can provide insight into the nature of problems and make recommendations for solutions based on their specific knowledge and understanding.

During the research investigation, at least one (one) important informant was present to provide updated technical information on Information Security.

#### **4.4.3 Secondary Data**

Secondary data was used in some of the research tasks, such as identifying and assessing various governmental/international policies, plans, acts, documents, guidebooks, journals, seminar papers, web resources, and so on.

### **4.5 Data Interpretation**

Employees were given e-mails, and the replies to a questionnaire from a total of 21 participants were obtained for this study.

In a research project, data analysis entails summarizing a large amount of data and presenting the results in a form that corresponds to the most significant features. This requires a process called content analysis. Content analysis involves coding and classifying data. The procedure involves a series of steps-

- Read the transcript thoroughly and make a brief note about the nature of information.
- Look through notes and find the differences
- Categorize items based on content
- Search for the link among the categories
- Divide the categories of data into major and minor heads by comparing and contrasting
- Highlight items of data with their categories in the transcript
- Collect all the extracts from the transcribed interview
- Review the data within the system of categorization
- Look at the range of categories whether close categories fit together
- Get a clear-cut theme

#### **4.6 Validity and Reliability**

The goal of a full-fledged research project is to be valid and dependable in terms of data collecting, analysis, and other aspects. This is true of my research as well. Validity is defined by Kirk and Miller (1986), as referenced by Kitchen and Tate (2000), as the degree to which survey findings are correctly understood, while reliability is defined as the degree to which research findings are independent of any incidental circumstances. Also, according to Gorbich (1999), validity is the capacity to verify a study's outcomes against its stated objectives.

#### **4.7 Problems, Challenges and Limitations**

Every empirical study has specific constraints or problems that must be overcome during the data collection procedure. Offices in Dhaka city, for example, were closed for semi-structured interviews owing to government-imposed lockdown, except for a few. It was challenging to conduct face-to-face interviews while adhering to the Covid-19 protocol. Furthermore, several respondents were not at their workstation. All these obstacles could influence the study's outcome in some way. The research, on the other hand, attempted to overcome all these obstacles and offer as accurate a picture of the research topics as feasible.



## **CHAPTER V: ICT PERSPECTIVE FOR INFORMATION SOCIETY**

### **5.1 Overview of the Progress**

This research defines the Government organizations as the part of the Information society that requires an Information Security because Government organizations holds the access to public's private and confidential information therefore maintenance of such information security is an important perspective that must be well-thought-out.

The "Digital Bangladesh" concept proposed by the Government of Bangladesh entails with the goal of enhancing people's lives, safeguarding people's democracy and rights, openness, accountability, establishing justice, and ensuring that government services are delivered to citizens' doorsteps via technology. Digital Government, Human Resource Development, IT Industry Promotion, and Connecting Citizens are the four pillars of Digital Bangladesh. Bangladeshi youth are being benefited from the use of digital technology, which is driving economic growth and social wellbeing. Consumer spending in the ICT sector is over USD billion and expanding at a rate of approximately 6% per year, with a market of more than 160 million people. As a result, Bangladesh has a bright future in the ICT sector.

Bangladesh, like other growing Asian countries such as India, China, and Malaysia, is eager to take advantage of the Digital Age's potential and catch up with technologically advanced countries. Bangladesh is presently investing in IT areas and should continue to do so, reaping significant benefits in terms of more employment and income, as well as faster growth. The Bangladesh government is producing thousands of jobs for Bangladeshi youth as the ICT sector continues to flourish and countless new IT companies emerge, reducing the country's unemployment crisis. The government is recruiting foreign corporations to set up shop in Bangladesh by investing in IT parks, bringing billions of dollars in investment and creating thousands of new employments. As a result of the recent boom in the sector, Bangladesh is poised to take advantage of all digital technology's growth potential and catch up faster with high-income countries.

The government's commitment to build 'Digital Bangladesh' has been on progress to be fulfilled for the last decade. Bangladesh is widely acclaimed today in the world arena for smooth flow of information and formation of a technology-efficient society.

In continuation of this, unprecedented success has been achieved in development and modernization of post and telecommunication. The tremendous development of Bangladesh has been led by the proper guidance of the nation's leader- the Government of Bangladesh. The Government has looked at every possible way to enhance the country's position. Bangladesh is adapting, mixing, and acquiring resources in order to meet future digital jobs while recognizing the consequences of digitization. Bangladesh is prepared to fulfill global demand with technology-driven skills. It is one of the top ten tech gadget growth markets, with a large customer base that is quick to accept new technologies.

On May 12, 2018, Bangladesh successfully launched "Bangabandhu Satellite-1" into orbit. Bangabandhu Satellite-1 boosts the nation's economy by providing all citizens with a variety of telecommunications services (direct-to-home TV, radio, telemedicine, education and internet access). The launch of Bangladesh's first telecom satellite, which will enable it to demonstrate its independence in this industry and offer communications and broadcasting services to a few neighboring nations, including Nepal, Myanmar, and Bhutan, was eagerly anticipated. The country currently has a 99.68% tele density rate and a 64.9% internet density. Besides, the number of mobile SIM subscribers is 16.84 crore and the number of Internet subscribers increased to 11.06 crore. Revenue collection of the government through the Post and Telecommunication division was Tk. 5,156.70 crore in FY 2019-20. Bangladesh Telecommunication Regulatory Commission (BTRC) was implementing the project in collaboration with Space Partnership International, LLC of the United States.

In order to provide high-speed mobile Internet services, 4G service has been introduced besides the 3G network. At present, the number of 4G subscribers has increased to 1.17 crore. A roadmap has been crafted with a view to launch 5G internet service network in the period of 2021-26. Bangladesh officials says that they have been paying their attention to work on 5G and utilize the advantages. Data rates in 5G can exceed 10 Gbps, which is over 100 times faster than 4G. Furthermore, a command on a 4G network takes 50 milliseconds to react; whereas a command on a 5G network takes less than one millisecond to answer. Countries such as China, Japan, the United States, the United Kingdom, Switzerland, and the Philippines have already implemented 5G networks. Aside from that, several countries, including India

and Australia, are developing their own 5G networks. In partnership with state-owned mobile operator Teletalk, BTRC unveiled the first 5G network in Bangladesh on December 12, 2021, at the Radisson Hotel in Dhaka.

In addition to Southeast Asia-Middle East-Western Europe-4 (SEA-ME-WE-4), Bangladesh has been connected to the SEA-ME-WE-5 submarine cable consortium, which increases the country's bandwidth capacity. The Southeast Asia-Middle East-West Europe 4 (SEA-ME-WE 4, SMW4) undersea cable connects Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, the United Arab Emirates, Saudi Arabia, Egypt, Italy, Tunisia, Algeria, and France across a distance of roughly 18,800 kilometers. The second submarine cable landing station has also been installed in Kuakata. Installation of the third submarine cable landing station is at the final stage. Presently, the bandwidth capability of the submarine cable is 1,800 Gbps and the use of submarine bandwidth increased from 7.5 Gbps to 618 Gbps in the last 10 years. Growing use of bandwidth across the country has now gone up to 950 Gbps. Along with submarine cables programs have been adopted to establish international terrestrial connection. The price of per MBPS bandwidth was Tk. 72,000 in 2008, which has now been shrunk to Tk. 420 which is reduction of a greater portion.

Crime is a big worry in today's communities, and it has a wide-ranging impact on peaceful coexistence. Any preventive measure or policy that lessens, prevents, or ends victimization by crime or violence; this includes both public and private initiatives to lessen victimization rates as well as public and private initiatives to lessen victimization rates; it also includes government and non-government initiatives. Crimes committed using mobile phone technologies have reduced significantly due to the introduction of biometric SIM registration. Government has restricted every individual to use biometric registered SIM as various crimes like threatening, abduction, blackmailing, extortion, contract killing, fraud etc. used to occur by the help of unregistered mobile phones. Many individuals often contained multiple contact numbers and carried illegal activities by such usage. Legal actions are also being taken against illicit business operators using VOIP technology and actions are taken against filed complaints by victims. All criminal activities are now taken in consideration and attempted to reduce in number by working on those.

International services such as international recharging, e-ticketing, inward remittance flow, utility bill payment, mobile banking, etc. have been introduced with the help of mobile financial services. Without the use of a bank branch, a banking procedure can be used to provide financial services to unbanked areas in a timely and cost-effective manner. To provide banking and financial services through mobile technology devices, such as cash-in, cash-out, merchant payment, utility payment, salary disbursement, international remittance, government allowance distribution, and ATM money withdrawal. Now, public pays their bills and other payments through the different financial application services. Some common examples are school fees, tuition fees, electricity bill, gas bill, shopping, bank payments and a lot more. It has reduced the necessity of standing in long queues, wastage of time and money. Most of the bank related works can be done by Internet Banking reducing the need to visit the banks frequently. During the COVID-19 pandemic period, such advancements were of great use, people remained in the houses and perform the necessary works without the need to go outside. Technology and its adaptation have made life easier now a days. Mobile network has been launched in south-eastern three hill districts of the country. A project to build network in inaccessible, remote and island areas is also being implemented. Almost every individual within the country has access to at least one mobile phone.

Teletalk Bangladesh Limited is a company based in Bangladesh. Teletalk, Bangladesh's only state-owned GSM, 3G, LTE, and 5G mobile phone operator, began operations in 2004. Teletalk has a customer base of 6.27 million as of August 2021. It also offers a comprehensive set of digital services. Through the government owned mobile phone company Teletalk, arrangements have been made for receiving applications for various public examinations, payment of tuition fees, distribution of examination admit cards, information about seat arrangements, location and exam results. Besides, education board registration process for the students of SSC and HSC is being done through Teletalk. In a word, almost all the public institution's activities can be performed via Teletalk network. The effort of physically visiting to institutions and carrying out the activities has reduced to a great extent. These enhancements brought peace, relaxation and hassle less life for public.

Bangladesh's emergence of e-commerce is older than previously considered. Our country witnessed a small version of e-commerce in the late 1990s to service NRBs

looking for ways to send gifts to Dhaka. From 2000 to 2008, the adoption of e-commerce was extremely slow. There were several flaws in the payment gateway, shipping system, and client education regarding e-commerce at that time. E-commerce grew in popularity in the country after the launch of SSL COMMERZ in 2010. When *akhoni* and *ajkerdeal*, two ecommerce sites, were presented to online users in 2012, the situation began to shift. Customers have reacted well to it, notably in Dhaka. Bikroy.com is an example of a company that takes a unique approach to business. Groceries and other industry items have also made an appearance, with sites like othoba.com, pickaboo.com, and chaldal.com representing their respective fields. In Dhaka and Chittagong, Hungry Naki and Food Panda are two well-known food and grocery delivery e-commerce services. As a result, e-commerce is becoming more popular by the day.

E-commerce, cash, speed post, post money, etc. have been introduced through modernization of postal services. Internet services are being provided at 8,500 digital post offices and facilities for remittance flow from abroad are being ensured. Several 118 vehicles were provided at the field level in order to strengthen the postal services. The Bangladesh Post Office has begun delivering shipments for online marketplaces on a larger scale across the country, marking a significant step forward in the country's e-commerce development. The postal agency has begun delivering roughly 500 orders every day for the country's renowned online platforms, after two and a half years of preparations.

BGD e-Gov CIRT was founded under the Ministry of Posts, Telecommunications, and Information Technology to work on the incidents in order to strengthen the country's entire cyber security infrastructure and predict future probable assaults by analyzing current attack trends. BGD e-GOV CIRT also undertakes research and development projects based on security threat challenges and vulnerabilities observed in order to improve future threat detection policies and reduce threat detection time. The BGD e-Gov CIRT throughout organized several interactive training sessions. The followings are given below:

- For iBAS++, BGD e-GOV CIRT organized a five-day training on "Information Systems Audit."

- Bangladesh Army received three days of training from the BGD e-Gov CIRT on "Basic Cyber Security."
- Bangladesh Army received four days of training from BGD e-Gov CIRT on "Cybersecurity and Secure Computer User."
- Bangladesh Police received five days of training from the BGD e-Gov CIRT on "Information Systems Audit."

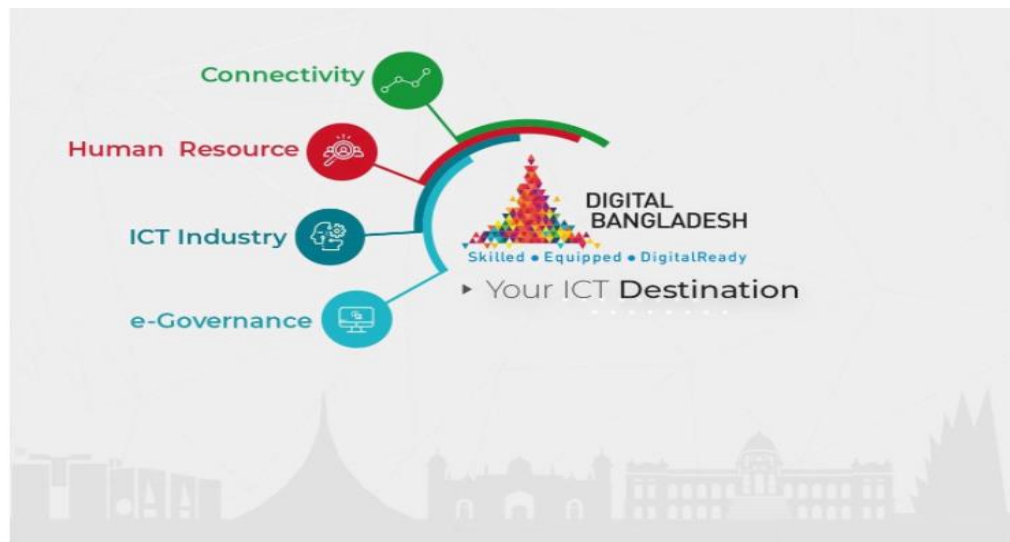


Figure 5.1 Four pillars of Digital Bangladesh

Source: <https://archive.dhakatribune.com/business/2020/12/13/how-digital-is-bangladesh-after-eleven-years>

Through BTCL, fiber optical cable has been set up in 30,100 km to connect 1,216 unions of 478 upazilas of 64 districts with a view to provide broad band internet connection. An opportunity has been created for 1.39 lakh new telephone connections by replacing 1 lakh old analogue system by BTCL's own funding. There has been an effort to facilitate internet-based education, high speed broad band and WI-FI connections were installed in 587 government colleges/ universities and training institutions throughout the country. Apart from these, several projects titled 'Modernization of Telecommunication Network for Digital Connectivity', Switching and Transmission Network Development for Strengthening Digital Connectivity, Installation of Telecommunications Network at Mirsharai 84 Economic Zone in Chattogram' are at the final stage to be implemented. In addition, the BTCL has announced plans to connect all upazilas in Bangladesh to a fiber optic network by 2023, enabling 5G services. Without fiber optic networks, the internet of things (IoT), smart device proliferation, cloud computing, and self-driving cars would not be possible. The country's leading telecommunications provider will lay an additional

1,300 kilometers of fiber optic cable, bringing the total length of fiber optic cable in the country to 35,000 kilometers. The country will be divided into eight clusters for the purpose of laying 1,000Gbps, 800Gbps, and 600Gbps fiber optic cables to assist mobile telecom operators with the seamless rollout of 5G service in the country and to assist the country in reaping the benefits and functions of 5G technology. Bangladesh Telecommunications Provider Limited (BTCL), a state-owned telecom company, wants to develop its fiber-optic network to provide better broadband coverage and uninterrupted telecommunication services across the country. The corporation has proposed a project to the Planning Commission with a cost of Tk. 1,059 crore and a four-year deadline.

A facility has been created for subscribers for working through the launched Dot BD (.bd) and dot bangla (.bangla) domains. Bangladesh's Internet country code top-level domain (ccTLD) is.bd. The government unveiled the national online portal, which includes 25,043 sites from various government agencies. On the International Public Service Day, the portal [www.bangladesh.gov.bd](http://www.bangladesh.gov.bd) was launched with over two million materials to ensure transparency and accountability in government activities. The Ministry of Posts, Telecommunications, and Information Technology oversees it. The Telephone Shilpa Sangstha Limited (TSS) has been capacitated to assemble and market laptops and computers at affordable prices in the country. Besides, land telephone sets, mobile phones, tabs, mobile batteries and chargers, digital electric meters are being produced and marketed locally. Prices of the products produced locally are kept reasonable to make it available for greater portion of the population. Educational needs can easily be satisfied by such attempts.

Optical fiber and copper cable produced by Bangladesh Cable Shilpa Sangstha Ltd.; Khulna has gained the capability to meet the demand of the country. The Information and Communications Technology Division (ICTD) has taken and implemented diverse initiatives to expedite implementation of 'Digital Bangladesh'. The division has initiated different development projects including launching projects and programs and formulating laws and guidelines with focus on four objectives including building ICT infrastructure, developing skilled human resources, e-governance and industry promotion. Digital Bangladesh has given rise to a new face of Bangladesh with remarkable advancements in terms of technology as well as economy.

The democratic government has declared "Digital Bangladesh" as its "Vision 2021," which includes through the most efficient use of technology, ensuring people's democracy and rights, transparency, accountability, creating justice, and ensuring delivery of government services to every door—all with the goal of enhancing the general public's everyday livings. There are four pillars to Bangladesh's digital transformation. Digital Government, Human Resource Development, Promotion of the IT Industry, and Citizen Connectivity. To create a 'Digital Bangladesh', the remarkable activities taken by the ICT Division are mentioned below:

- The Bangladesh Computer Council (BCC) has officially established world 8th largest Uptime Certified National Data Centre (Tier-4) at Bangabandhu Hi-Tech City, Gazipur. A total of 58,095 web mails and email accounts have already been opened in 492 domains and more than 25,000 official websites and 260 applications have been hosted there. Many government enterprises already hosted and collocated their datacenter in the Tier-4 National Datacenter (NDC) premises. One disaster recovery center also had been established in Jessore.
- Several districts have been chosen for the operational purpose of the Hi-tech Park such as Sylhet and Rajshahi and invested around 66000 lakh takas. Additionally, the government has invested in several training, information, and incubation centers around the country. Another project of Bangladesh Hi-Tech Park authority that is Bharot Digital Service and Employment Training (BDSET) Center Project Information. The project includes ToT training for around 30 persons in India in emerging technology, professional training for about 2400 people in IT/ITES related subjects in Collaboration with Indian Government.
- In the mobile sector, the government made several significant moves, including bill payment via mobile, port automation, e-center, introducing e-governance (partially), getting public exam results through SMS and providing information about the university admissions procedure via SMS
- Bangladesh Bank (BB) has been given permission to conduct online money transactions, pay utility bills online, transfer cash (account to account), accept payments for selling goods and services, and accept online credit card payments in local currency.



- In Submarine Cable: Bangladesh's government has already made steps to connect the country to the second Submarine Cable Network, ensuring safe connectivity to the information superhighway.
- In terms of ICT policy, the government passed a national ICT policy with help from the Prime Minister's Office's access to information program. The government has made steps to encourage ICT in all parts of society, including hard-to-reach places, tax and tariff reductions on computers, and promotion of ISP services, among other things.
- In terms of education: SSC and HSC results were made available via mobile and internet since 2009, as well as being emailed to educational institutions. Various schools and institutions have begun the process of offering laptop and internet connectivity. Shahjalal University of Science and Technology completed its entrance registration procedure using data from education boards and mobile phone-based applications. The results of medical college and primary examinations were made publicly available for the first time.
- Providing high-quality training to young people in order to increase the number of IT experts to 2 million by 2021. To achieve the goal, it has built specialized labs and launched projects and programs. Compulsory secondary education has also been implemented by the government.
- In the field of health, the country's 800 health clinics now have access to the internet and mobile phones. A few telemedicine centers have been established. The government is establishing community e-centers/tele-centers across the country to ensure that everyone has equal access to technology. There are already over 2,300 of them. Now, rural areas of Bangladesh contain the opportunity of various medical treatments
- Honorable Prime Minister Sheikh Hasina launched the much-anticipated Machine-Readable Passport (MRP) and Machine-Readable Visa (MRV) on Wednesday (3 June 2010), putting Bangladesh one step closer to becoming a Digital Bangladesh. In Bangladesh, the transition from machine-readable passports (MRP) to electronic passports (e-passports) began in 2019. The e-passport is a biometric passport with a microchip containing the passport holder's personal and biometric information. This move is intended to improve the security and integrity of the passport issuance process, as well as to combat

identity fraud. A polycarbonate data sheet, laser engraving, and an implanted electronic chip are among the sophisticated security elements of the e-passport. These elements make counterfeiting harder and protect the identity of the passport bearer. By 2023, the Bangladesh government hopes to have completed the transition from MRP to e-passport. The government has also installed multiple e-gates at international airports in Dhaka, Chittagong, and Sylhet to allow the easy admission and exit of e-passport holders. In Bangladesh, the move from MRP to e-passport is a crucial step in improving passport security and preventing identity fraud.

- The government has given emphasis on research and development-based education under that great initiative the Ministry of Education implemented Bangladesh Research Education Network (BdREN) project supported by the World Bank and implemented by The University Grants Commission of Bangladesh (UGC). The project had been established in the aim of enhance quality of Higher Education with collaboration of different university, institute, professor and students in home and abroad. The BdREN's multi-gigabit capability aims to link all educational, scientific, and research institutions in Bangladesh, as well as libraries, labs, hospitals, and agricultural organizations, in order to give academics, scientists, and researchers who are dispersed across the country dependable access to resources. The initiative is funded by an International Partnership (IP) collaboration with several universities and research networks in the United States. IP is introducing The Bangladesh Brain Bank Initiative, a series of activities that will connect professors and specialists in the United States to deliver lectures, workshops, and seminars on a variety of issues to Bangladeshi students and academics.
- As many as 18,434 government offices have been connected under a single public network and along with that, 254 Agriculture Information Centers, 25 Telemedicine Centers, ICT Career Camps and establishment of BGD e-Gov Computer Incidence Response Team (CIRT) have been established to implement e-governance. The Info Sarkar (3rd phase) Project has connected 1,700 unions through a fiber-optic cable network.
- Around 2,936 government officials have been offered training on e-governance and cyber security at home and abroad. To implement the "Digital

Bangladesh" goal effectively and efficiently, the government has started the Master Plan for Digital Bangladesh Project.

- In the Technical Category of Public Administration Award, Bangladesh Computer Council has achieved the Public Administration Award 2017, the ICT Education Award-2017 from Asian–Oceania Computer Industry Organization (ASOCIO), the Digital Government Award-2018, e-Asia-2017, the Open Group President Award-2018 and the WITSA Award 2017.
- The Bangladesh Hi-Tech Park Authority has taken an initiative to build 28 Hi-Tech Parks across the country. Sheikh Hasina Software Technology Park at Jashore has already been established. Operation of the Janata Tower Software Technology Park with 72,000 square feet space at *Karwan Bazar*, Dhaka has already in full swing. Moreover, establishment of Hi-Tech parks in 12 spots including Rajshahi and Sylhet is in progress.
- By this time, Total 45,480 people have been trained up at different Incubation Centers and IT parks of the country including Sheikh Kamal IT Training and Incubation Centre at Natore.
- “Information on Digital Entrepreneur and Innovation Ecosystem Development Project”-
  1. To construct Vision 2021 Tower-2 at Kawran Bazar, a new building with climate-resilient and sustainable infrastructure will be developed.
  2. To develop an effective innovation eco-system by improving the environment of existing STPs and Innovation Hubs in renowned institutions.
  3. To establish common facilities for researchers, start-up students, and businesses to use.
  4. To boost digital startups' and small and medium-sized businesses' market entry and growth rates in the digital economy.
  5. To foster a gender-balanced digital entrepreneurship culture.
- Employment opportunities for 12,079 people have been created in the Hi-Tech Park and Software Technology Parks of the country.
- Seminars/workshops have been organized in all around the country for government officials on the ‘Use of Digital Signature Certificate and Cyber Security’. Different government and non-government organizations and banks

have already initiated their own websites and started using digital sign in their offices. The Election Commission has set up a connection of NID database through VPN to verify the citizens' information. Along with the advancements in technology, the government has kept considerable priority upon training its IT officials/employees through seminars/workshop ensuring skill and knowledge development.

- In Bangladesh, electronic voting machines (EVMs) were developed to address issues with paper ballots. They were initially successfully employed in 2007 for the election of the Dhaka Officers' Club's working committee. EVMs have been utilized sparingly in several city corporation elections throughout the country since then. For the first time in a general election, they were used in six constituencies in 2018. EVMs are basic electronic devices that record votes instead of the ballot papers and boxes that were previously utilized in traditional voting systems. It's a straightforward machine that both poll workers and voters can simply operate. Nobody can interfere with its programming and influence the output because it is a standalone machine with no network connectivity. It primarily consists of two units: a control unit and a ballot unit. The Control Unit is the key unit that holds all data and regulates the EVM's operation.
- Awareness-raising workshops for women titled 'Cyber Security Awareness for Women Empowerment/Digital Security Awareness for Girls' in different education institutions of all divisions and districts have been organized. Training on Cyber Security has been given to 26,500 girls in these awareness-raising workshops. Women of Bangladesh has been showing remarkable progress in each of the sectors.
- A total of 7,931 digital education labs have been set up in different education institutions all over the country. There are 4,176 Sheikh Russel Digital Labs, 3,579 computer labs, 21 university IT labs, 100 Sheikh Russel digital classrooms and in Saudi Arabia 15 Sheikh Russel digital labs. Many universities now also contain Virtual laboratories.
- As many as 200 types of digital services are being provided to people in general after setting up 5,737 digital centers. The world's biggest web portal

‘Information Window’ consisting of 25,000 websites has been introduced which is internationally admired and awarded.

- Total 44,391 people are given training from ICT division to build skilled human resources in IT sector. There are 32,684 youths, 11,036 women and 671 people with special needs among them. According to a survey conducted by the Oxford Internet Institute, Bangladesh is ranked 2nd based on online workers (freelancing) in the world. Export in the digital sector has risen up to US\$ 800 million from US\$ 2.6 million.
- Bangladesh has surpassed many other countries as one of the best venues for freelance online job. Dhaka is ranked third among worldwide locations where internet employment is outsourced from the west, according to oDesk Corp, a leading marketplace for companies and online employees based in the United States. Freelancing outsourcing jobs employ approximately 5 million freelancers are involved in outsourcing.
- A total of 804 Videoconferencing Systems have been set up in the whole country and Union Digital Centers have been built using solar power in 1,013 unions without electricity.
- Bangladesh has shown success in organizing Asia-Pacific Information Superhighway (APIS) Steering Committee Meeting, BPO Summit Bangladesh, Women ICT Frontier Initiative (WIFI) and APCICTA Awards 2017.
- Tax Holiday has been announced for the investors for up to 2024 in Hi-Tech Park.
- Information and Communications Technology Adviser to the Honorable Prime Minister Mr. Sajeeb Wazed Joy was awarded ‘ICT for Development’ award at the 71st conference of UNO held in 2016 for his special contributions to the IT sector to build up ‘Digital Bangladesh’.
- The Fourth Industrial Revolution and Beyond International Conference was held in Bangladesh at the University Grants Commission (UGC) (IC4IR 2021). By utilizing artificial intelligence, the internet of things, data analytics, and cloud computing to address industrial difficulties, the UGC aspires to establish a prominent international forum for academics and professionals from a variety of fields to share cutting-edge research findings. Through the

exchange and promotion of best practices, IC4IR 2021 promotes the sharing and dissemination of creative and useful developments in techniques and technologies with industrial applications. The conference will include topics such as signal and natural language processing, artificial intelligence, robotics and automation, IoT and smart agriculture, data analytics and cloud computing, communication and networks, and more.

- Aspire to Information (a2i) program, in the meantime, has initiated a number of remarkable programs such as Union Digital Centers, 333 Call Centers, Service Process Simplification, Land Services, Digital Service Accelerators, Innovation and Culture in Public Service, Multimedia Classrooms and Digital Contents, National Portal, Digital Financial Inclusion, District Branding, Rural e-Commerce, Idea Bank, Service Innovation Fund, ‘*Muktopaath*’ e-Learning Platform, Mobile Keypad Standardization and SMS in Bangla, and South-South & Triangular Cooperation, etc. Research findings showed that these initiatives of a2i saved time up to 1.2 billion, US\$ 4.7 billion in cost and 627 million visiting time of the citizens. The success of these initiatives is being awarded by different organizations at home and abroad. Remarkable achievements are the UN South-South Cooperation Award 2018, Sohel Samad Memorial Prize 2018, ‘International Invention, Innovation & Technology Exhibition’ (ITEX) Award 2018, WSIS Award by *Muktopaath* 2018, President Award 2017 by Open Group of India, President Award 2018 for ek-Sheba system, etc.
- Fellowship and scholarship offer for researching on ICT and the Subsidy Policy for Innovation, 2017, the Government Email Policy, 2018, and the Digital Security Act, 2018 are in place through gazette notifications. Gazette notification of National Information and Communications Technology Policy, 2018 has already been done.
- During FY 2013-14 to FY 2017-18, Tk. 10.41 crore was provided as fellowship and scholarship for 249 students/researchers, who are doing masters/MPhil/PhD or postdoctoral studies in different universities at home or abroad.
- Seven MoUs have been signed with China, India, Sri Lanka, Cambodia and Singapore for cooperation in connection with ICT expansion.

## 5.2 Achieving SDGs

ICTD has been playing an important role with a view to achieve Sustainable Development Goals (SDGs). Computer science topics such as Environmental Informatics and Computational Sustainability contribute to the development of sustainable ICT. The Sustainable Development Goals, often known as the Global Goals, are a set of 17 interconnected global goals aimed at providing a "blueprint for a better and more sustainable future for all." As a result, the SDGs are aimed at achieving a number of life-changing "zeros," such as zero poverty, hunger, AIDS, and discrimination against women and girls. The agenda includes 17 Sustainable Development Goals (SDGs), which are further developed into 169 goals that address economic, social, and environmental issues. The 17 Sustainable Development Goals are:

1. GOAL 1: No Poverty
2. GOAL 2: Zero Hunger
3. GOAL 3: Good Health and Well-Being
4. GOAL 4: Quality Education
5. GOAL 5: Gender Equality
6. GOAL 6: Safe Water and Sanitation
7. GOAL7: Affordably Clean Energy
8. GOAL 8: Decent Work and Economic Growth
9. GOAL9: Industrial Productivity, Innovation, And Infrastructure
10. GOAL 10: Reduced Inequality
11. GOAL 11: Sustainable Cities and Communities
12. GOAL 12: Responsible Consumption and Production
13. GOAL 13: Climate Action
14. GOAL 14: Life Below Water
15. GOAL 15: Life on Land
16. GOAL 16: Peace and Justice Strong Institutions
17. GOAL 17: Forming Partnerships to Achieve the Objective

In five ways, the SDGs achievement can be met with the contribution of ICT:

1. Information and communication technology (ICT) expands quickly, as evidenced by the fact that mobile phone subscriptions surpassed seven billion in 2015. Can relate to increase in industrial productivity, its innovation and infrastructure. Expansion of the ICT can reduce the number of unemployment, as a result reducing the poverty.
2. ICT can assist save money in a variety of industries, including health care, banking, and education producing sustainable cities and communities, as a result a stepping towards a proud nation.
3. Information and communication technology (ICT) can assist in raising awareness of new technologies. Unlike in the past, knowledge on new technology may now be disseminated at breakneck speed via social media, mobile devices, and other electronic means.
4. New applications are being enhanced and upgraded as a result of national and worldwide information flows.
5. Using ICT, low-cost online platforms for training workers in new technologies can be built.

By this time Planning Division of Bangladesh government has formulated a well-articulated SDG mapping which indicate precise responsibilities to be carried out by different Ministries/ Divisions/ Departments or subordinate offices for materializing the targets of SDGs. In this connection, ICTD is assigned to perform necessary actions for realizing goal 1, 4, 5, 8, 9 and 17. Among those goals, ICTD is the lead ministry for target 9 (c) and 17.8, Co-lead for 9(b) and associate for 1.3, 1.4, 4.4, 4.7, 5b, 8.1, 8.2, 8.3, 8.6, 9.2, 9.5, 17.6, 17.16 and 17.18. This office has been endeavoring to attain these marks on time.



In order to accomplish 9(c), the entire Bangladesh has come under mobile phone network. Right now, approximately 80% population of the country has access to at least one mobile phone network. Goal 9(b) acmes impact on GDP by moderate and state-of-the-art industries. Bangladesh Bureau of Statistics (BBS 2018) confirms that ICTD has been trying to promote a knowledge base society. Department of ICT (DoICT) has been covered almost 60% surface area of Bangladesh with optical fiber network. It will let rural people to get easy, safe and low-cost access to the internet highway. It will also make the pavement to reach the target 17.8 within a very short span of time.



Figure 5.2 Realization position of SDGs by the ICTD

*9(c) By 2020, greatly improve access to information and communication technology, with the goal of providing universal and inexpensive internet access in LDCs.*

- 2300 union parishads have been brought under optical fiber connectivity, establishing connections with rural areas of Bangladesh that had been previously disconnected.
- 990 police stations have been brought under VPN.
- 25 institutions under 03 (three) unions of Moheshkhali upazila have been brought under high-speed internet connectivity.
- Tier-IV data center has been established with upgraded 03 (three) peta-byte storage capacity.
- 06 (six) ICT resource centers have been established under BCC monitoring and 188 audio-visual tutorial content have been developed for physically challenged persons.
- A highly technical team has been formed in order to monitor Certifying Authorities (CA) activities. In this regard, CA monitoring project has also get approved by the Planning Commission, Bangladesh.
- PKI system has been upgraded and implement in every 03 (three) months. A public key infrastructure is a set of roles, policies, hardware, software, and procedures for creating, administering, distributing, utilizing, storing, and revoking digital certificates, as well as for managing public-key encryption.
- E-stamping project is under consideration by MoF
- Women involvement in ICT eco system has accomplished by providing training in three different components-
  - i) Freelancer to entrepreneur
  - ii) IT service provider and
  - iii) Women agents in call centers

Approximately 4000 HSC and above level women are provided of freelancer to entrepreneur and same number of women has trained on IT service provider. 2500 women are trained on call center agent.

- With a view to establish digital connectivity project, a MoU has been signed between DoICT and CRIG. In the upcoming PEC meeting, the DPP will be recast, and the project will be in place within the stipulated time.
- A tripartite MoU is signed among ICTD, ERD and Embassy of Denmark in Bangladesh to conduct a feasibility study on (proposed) digitalize islands, *haor* and *bill* areas.
- 5875 specialized digital centers have been established. Those centers provided a wide variety of government services to the grass root people. They are taking services like- submission of online passport applications, paying passport fees, getting public exam results, online NID copy, job application, communicate with the expatriate relatives through video conferencing, photocopy, print, compose, download and many more.
- 333 call service centers are being operated in 64 districts. People are taking advantages of those centers by calling for emergency help which are social in nature, even people can get emergency food assistance from government through this service.
- 999 call service initiated for emergency helplines. Public are being benefited in case of emergency as they request for help.
- *Krishibatayon* (Agricultural portal) have been developed for agricultural farmers. Almost 8 (eight) million farmers meanwhile have received services and empowered with the knowledge of production technology, quality foods, existing demand and market price of their products which ultimately formed a virtual bridge between urban and rural areas in Bangladesh.
- Government has been made payment to the distressed people within social safety net program through digital system and thus ensure helping the right person in need. Even in the period of COVID-19, payments and foods were distributed among the people in need to save them from hunger as during COVID-19, all the offices or institutions remained closed. It has been figured that many people lost their jobs during COVID-19 as the organization's financial state has been affected by the pandemic.

- The digital financial service is a joint venture between the Bangladesh Bank and a2i which has made possible agent banking which aims to broaden and deepen digital financial inclusion by Citizen-centered product and service innovation. In most emerging markets, the trend is to merely alter financial products and services developed for the wealthy and try to sell them to the poor, who don't understand or need them. In addition, Payment's digitization is also included in the list

*17.8 By 2017, fully operationalize the technology bank and the scientific, technology, and innovation capacity building mechanism for LDCs, and increase the use of enabling technology, especially information and communication technology.*

- 100 tech-innovation based startups were funded and supported by ICTD
- Funds provided for different government projects, as well as innovative ideas proposed by the graduate students within the country.
- Digital forensic labs have been setup and operationalized in order to prevent cyber-crime and provide evidence-based proof to the cyber tribunal.
- A good number of workshops and seminars have been conducted across the country to achieve digital security awareness and avoid cyber bullying for several thousand girls. Cyber bullying has led to increase suicidal rates within the country therefore, necessary measurements are being taken, complaints filed and executed rapidly to decrease the effect of the circumstances. Special section of Bangladesh Police involved in cyber bullying cases to resolve problems at its earliest.
- 4016 Sheikh Russel Digital lab and classrooms have been setup in different educational institution for providing language training for the exodus people
- 137 Public universities are connected:
  - Innovations are fostering
  - Projects on Robotics, AI have been adopted
  - 5350+ online proposals submitted

- Virtual laboratories
- Well modified curriculum to maintain international standards
- 100<sup>+</sup> individual organization and 50<sup>+</sup> student/ teacher researchers of universities are getting funds every year both national and international.

Expansion of ICT in Primary Education:

- In order to set up digital classrooms, 58,921 laptops and the same number of multi-media projectors and sound systems with internet connections have already been provided to 50,416 government Primary Schools,
- A total of 800 officers and 1,05,755 teachers have been trained in ICT,
- 509 ‘Computer and Language Labs’ have been established in every upazila and metropolitan thana of the country in order to enhance the quality of the students by developing their technical and language skills.

Regarding digital security awareness, a lot of progress has already been made. Several groups in the country, including females, students, teachers, journalists, and government officials, have received training on cybercrime, concern legislation, social media security tactics, crime prevention measures, and particular protocols for filing complaints, among other topics. The CCA's office has created an online tool named 'Digital Evidence Management & Reporting System (DEMRS)' for the prevention of crime investigations and the early detection of offenders.

*9(b) in developing nations, support domestic technology development, research, and innovation, including by creating a favorable regulatory environment for industry diversification and commodity value addition, among other things.*

- 48 IT companies are running their business in Sheikh Hasina Software Technology Park, Jashore,
- 14 software companies and 10 startups are working in Janata Tower Software Technology Park.
- 6,00,000 square feet spaces ready for investment in Bangabandhu Hi-tech Park city, Kaliakoir.

- Basic infrastructure and land is ready at Bangabandhu Sheikh Mujib Hi-tech Park, Sylhet for investment.
- At Rajshahi's Bangabandhu Sheikh Mujib Hi-tech Park, a five-story structure with 72,000 square feet is ready to serve as a training and incubation center for investors.
- There are 12 (twelve) IT parks being built in various regions, 7 (seven) Sheikh Kamal IT Training and Incubation Centers, and an IT business incubator at Chattogram University of Engineering and Technology (CUET).
- Land development works for Bangabandhu Hi-tech City-2 project is going on covered 97 acres of land.
- 100 startups were funded 6.84 crore taka for establishment of an Innovation Design Entrepreneurship Academy.
- 5 (five) tools are under development for enhancement of Bangla language in ICT through Research and Development.
- There is an establishment on Software Quality Testing lab and Certification Center (SQTC). Quality testing of 30 software and 10 hardware items were done.
- A PDPP has sent to ERD for establishment of Japan-Bangladesh SET (Service, Employment and Training) Center.
- A world class PKI (Public Key Infrastructure) system is highly needed for ensuring Information security with digital signature certificates for online transaction and information sharing.
- With a view to floating development of mobile game and application skill project, by this time, 16,625 people have been given training and 8,525 people is engaged in IT related jobs.
- Through learning and earning development project training is provided to 38,660 people, 1 app development completed and 26 are under construction

### 5.3 Areas for further improvement for an Information Society

- ✓ Inadequate competent resources have repeatedly been identified as the single most significant hindrance. There are skill gaps at all levels of organizations and among people, including:
  - Basic ICT and smartphone knowledge of citizens, particularly people coming from rural areas. It can be increased through training sessions to help them develop skills or make them able to use such devices
  - Digital service design and execution
  - Business process renovation
  - Management of information centers and ICT systems in a safeguarded fashion
  - Integration, interoperability and information exchange between internal and external systems
  - Strategic ICT management and precaution.
- ✓ Inadequate impact for citizens: Few digital services have attained widespread adoption, and they often coexist with paper-based systems (adding cost and complexity to service delivery while benefiting only some users of the services).
- ✓ ICT duplication: Most government information systems run on different data centers, ICT architectures, and software development platforms, resulting in duplication requirements and investments.
- ✓ Lack of interoperability: Systems have primarily been designed in isolation from one another, making integration problematic. The National Enterprise Architecture and the E-Government Interoperability Framework are both little known, and those who are aware of them are unsure how to put them into practice in their ministries.
- ✓ Inadequate capacity with current shared services: Where BCC currently offers shared ICT services (such as hosting in the national data center, computer

emergency incident response), these services are welcomed but are unable to completely fulfill demand.

- ✓ Data protection, privacy, and cyber security: In the wake of the recent cyber security problems at Bangladesh Bank, agencies are becoming more and more aware of the need to strengthen the security of their digital government systems in order to shield the public administration from ongoing and evolving cyber threats, but they lack the necessary procedures, methods, and resources. Preventive approaches must be learned in order to stop future loss and harm to the country when terrorists develop new tactics and attacks.
- ✓ More seminars and webinars to increase employee collaboration and deliver ideas of Cyber security management as human factor is a major role in cyber security management. Top officials must monitor and control such processes and carry out the necessities.
- ✓ More collaboration of international conferences on Information technology to encourage talent minds to show their talents and such occasions can play roles of talent hunts for the country as well. This is also a representation of the country within the international ones.
- ✓ Offering more funds for research and development in the crucial sectors that are beneficial for the country. As like future developments on Artificial Intelligence and Machine Learning can lead to further development of the nation.

#### **5.4 Strategic direction adopted for Information Society**

The overall strategies are to-

- (i) Make the government a smart leader in the use of digital innovations to accomplish the goals of line ministries.
- (ii) The Bangladesh Cybersecurity Strategy for 2021-2025 has already been established by the Digital Security Agency, which is part of the Information and Communication Technology (ICT) Division. Officials from the ICT Division informed The Business Standard that the strategy will be presented to the cabinet for



approval soon, after making any necessary revisions based on feedback from other stakeholders (TBS).

- (iii) Improve the physical infrastructure supply side.
- (iv) Create interactive training sessions for employees to improve their skills in using the cyber security management system.
- (v) Through R&D, enhance knowledge generation and utilization, as well as human resources. It is possible to urge the private sector to use ICT technologies to solve competitiveness by allocating projects with adequate funding.
- (vi) Empower the ICT industry to increase investment and innovation in order to build global success stories, using the domestic market as a steppingstone.
- (vii) Develop digital technology-based redesign capabilities so that material and energy consumption, as well as waste, are reduced and yields are increased in everything Bangladesh produces.
- (viii) Leverage the digital economy to realize the fourth industrial revolution's potential and achieve the SDGs.
- (ix) Prepare for and benefit from the fourth industrial revolution as it unfolds.
- (x) Promote women's empowerment and advancements in the fields of work and education and
- (xi) Research and development in information technology to enhance the unfolding opportunities.

## **5.5 Creating an Information based Economy**

As part of its attempts to enhance the country's development in information technology sector and as well as economy, the government promotes the Digital Bangladesh plan. After 20 years of growth fueled by labor advantage, it is now time for Bangladesh to take use of vast technology, innovation, and

digital prospects to accelerate growth and achieve upper-middle-income status by 2031 and Information Society status by 2041. In keeping with 'Vision 2021,' the 'Vision 2041' has been adopted to give the nation's development dream a boost. By 2031, it seeks to eradicate absolute poverty and move into a higher middle-income status; by 2041, it seeks to do the same while progressing toward being a developed nation. Based on the experience of higher-middle- and high-income countries, provide all the services of a modern metropolis at the village level, turning communities into the focus of development. The Perspective Plan 2021–2041 was used to translate the goals and initiatives of the Vision 2041 into development plans. Democratization, decentralization, good governance, and capacity building are the four institutional pillars on which this approach is based. The people of Bangladesh will primarily benefit from this development and will also be the main forces behind its prosperity and transformation.

### **5.5.1 Digital Opportunities and Innovations**

Digital Bangladesh is an essential part of Bangladesh government's Vision 2021 and Vision 2041.

1. **Program on Aspire to Innovate (a2i):** The a2i initiative was formed in 2006 with UNDP help to spearhead the government's endeavor to transform Bangladesh into a Digital Bangladesh. By making policy decisions, implementing several e-Governance initiatives, directing and designating specific tasks to ministries and agencies, this project in the Prime Minister's Office has emerged as the true hub of Bangladesh's e-Government activities (**Aspire to Innovate Program**, 2020).
2. **National web portal:** A national web portal (<https://bangladesh.gov.bd/>) is a site where a country may showcase all its e-Government operations and direct users to desired connections all under one roof. In 2014, Bangladesh launched a national web platform. This site connects one to all of Bangladesh's administrative units, from the local to the national level. It has grown to become the world's largest public portal, with over 25,000 websites. Two million new articles and an e-directory have been uploaded to the Bangladesh

National Web Portal, including information on 700,000 government personnel and authorities (Access to Information Program, 2016).

3. **Bangladesh Form Portal:** Launched in 2015, the portal (<http://forms.mygov.bd/>) allows citizens to download, fill out, and submit any type of government form or application through a single web platform. This program, which is a big step toward e-Government, now has 1,400 forms, 1,200 of which are editable in PDF format and may be filled out. There will be more downloaded forms and online form submission options added in the future.
4. **Bangladesh Trade Portal:** In 2016, Bangladesh launched an online trade portal (<https://www.bangladeshtradeportal.gov.bd/>), the first of its type in South Asia, with the goal of providing a one-stop shop for export-import information to the business community. Anyone from anywhere in the world may now get basic information about conducting business in Bangladesh, such as an overview of the Bangladesh economy, existing merchant regulations and procedures, an import and export guide, and the process of starting a firm, among other things (The World Bank, 2016).
5. **Union Digital Centers (UDCs):** Widely regarded as a major e-Government initiative in Bangladesh, UDCs, which are positioned at the lowest levels of government, have become a portal to e-Services for the general public. By operating as a one-stop information and service delivery route, these centers decentralized the delivery of public services. One male and one female entrepreneur jointly run these centers, which use contemporary ICT to offer services like birth and death registration, exam registration, telemedicine, job applications, passport applications, mobile financial services, citizen certificates, photocopying, photography, computer composing, internet browsing, electricity and utility bill payment, job searches, and land records, among others. To date, 76.8 million citizens have received 323 million services through digital centers (Aspire to Innovate Program, 2018).
6. **Digital One-Stop Services** — Launched in 2018, *Ekseba*, *Ekpay*, and *Ekshop* are digital one-stop services that allow individuals to access a variety of government services, pay utility bills, and conduct e-commerce transactions online (Aspire to Innovate Program, 2019). *Ekseba* will act as a middleman, facilitating access to government services. It currently offers 162 services and

will eventually link to all three thousand. Citizens can use *Ekpay*, a one-stop payment site, to pay their energy bills, water bills, education-related fees, and other obligations. *Ekshop* is an e-Commerce platform that connects rural entrepreneurs with customers and industry stakeholders to make rural product marketing easier.

7. **Online Birth and Death Registration Information System (BDRIS)**: The government can keep track of every citizen thanks to the Online Birth and Death Registration Information System (BDRIS), which was introduced in 2010 and the **website link is - <https://everify.bdris.gov.bd/>**. This allows for the planning and delivery of all necessary services. The government states that 5029 register offices total across the nation, including 4571 union councils, 319 municipalities, 15 cantonment boards, 124 zonal offices of 11 city corporations, and 53 registrar offices of Bangladesh missions abroad that together make up a total of 5082 register offices, conduct online birth and death registration (Office of the Registrar General, Birth & Death Registration, 2000).
8. **e-Government Procurement (e-GP)**: To promote government procurement competency and openness. In 2011, a comprehensive e-GP solution was implemented (**<https://www.eprocure.gov.bd/>**). It is a web-based solution that tracks and manages the entire procurement process. A number of offices have already begun to use the e-GP. The system will be implemented across the board acquiring entities in a phase-by-phase manner. Tender applications and fees can be submitted by domestic and international potential tenderers via way of the procurement portal. e-GP is presently connected to 38 banks.
9. *e-Tathyakosh*: Launched in 2011, *Jatiyo e-Tathyakosh* is a national e-Content repository. It is Bangladesh's largest collection of contents on subjects such as health, education, agriculture, law and human rights, non-farm activities, disaster management, employment, science and technology, trade and commerce, and so on, with over 100,000 contents on 10,000 topics. (Aspire to Innovate Program, 2014) This online repository has evolved to serve as a single point platform for the distribution of livelihood information.
10. **e-Porcha**: Until recently, Bangladesh's land registration system was a remnant of the colonial era. The procedure of issuing any land-based document was difficult, costly, and time-consuming. The old system was replaced by E-

Porcha (<https://eporcha.gov.bd/>), which digitized land records and created an electronic system that made it easier for people to obtain papers (Aspire to Innovate Program, 2018a).

11. e-Health: The traditional system of health consulting has been supplemented by the availability of telemedicine services for the public. All government hospitals, from local to specialized, are furnished with a mobile phone and a web camera. The public can contact designated doctors for free medical advice, and patients at neighborhood hospitals can consult specialists through video conference (Hoque et al., 2014).
12. e-book: Since 2011, all basic and secondary level textbooks have been offered for free on the e-book platform.
13. e-TIN and Online Tax Payment: Electronic Taxpayers Identification Number (e-TIN) registration system and the online tax payment system (<https://secure.incometax.gov.bd/TINHome>) began in Bangladesh in 2013. Potential taxpayers can register, calculate and prepare tax returns, and submit them electronically.
14. *e-Krishi* (e-Agriculture): Recognizing the potential of ICTs in agriculture, Bangladesh highlighted e-Krishi by combining contemporary ICTs with conventional mass media to disseminate agricultural information. Farmers and other stakeholders may readily share essential knowledge and resources via e-Krishi.
15. Government to Person (G2P) and Person to Government (P2G): Efforts to automate the payment of the government's Social Safety Net programs began in 2018. There are currently 140+ programs throughout the country, administered by 23 Ministries and Divisions. Both the receiver and the government will save time and money by digitizing the manual payment method. From 2018, an effort called e-Challan was trialed to start the process of transferring a person's payment straight to the government treasury. Passport fees, national ID correction fees, and police clearance certificate fees can all be paid via e-Challan in addition to the traditional method (Aspire to Innovate Program, 2020a).  
Mobile Financial Service (MFS) is one of the ways used for G2P (Government-to-Person) payments, such as distributing social safety net allowances to recipients. MFS is a mobile payment system that allows users to

execute financial transactions using their phones. In Bangladesh, the government has started using MFS to distribute several sorts of G2P payments to beneficiaries, including social safety net allowances. To make these payments, the government has worked with mobile financial service providers such as bKash, Rocket, Nagad, and others. MFS payments provide various advantages over traditional payment methods, including better efficiency, lower transaction costs, and increased accessibility for beneficiaries, particularly those living in distant places. Furthermore, MFS can help to reduce the risks of fraud and corruption in G2P payments by guaranteeing that payments are delivered directly and securely to the intended recipients.

16. **COVID-19 Vaccination Registration Online Portal:** In Bangladesh, the COVID-19 Vaccination Registration Online Portal (<https://surokha.gov.bd/>) is a website where eligible persons can sign up to obtain the COVID-19 vaccine. Users must provide their personal information and choose a vaccination center before using the service. Users receive a confirmation message after registering and are informed of their vaccination date and time. The online site intends to simplify the vaccination procedure and ensure equitable vaccine distribution across the country.
17. **Made in Bangladesh "Meghna" Cloud:** Meghna Cloud is a cloud computing service developed by Meghna Group of Industries, Bangladesh's largest corporation. It is intended to provide Bangladeshi businesses and individuals with economical and dependable cloud computing options. Meghna Cloud provides a variety of services such as virtual machines, storage, and networking, as well as application development and deployment tools. The platform was created with open-source technology and is supported by a high-performance computer infrastructure. Meghna Cloud intends to increase cloud computing adoption in Bangladesh and encourage digital transformation across several industries.
18. **Boithok Virtual Meeting App:** Boithok (<https://vc.bcc.gov.bd/>) is a Bangladesh-developed virtual meeting program that allows users to hold video and audio meetings, webinars, and online events. It is accessible in both web and playstore versions for Android devices. The app has a variety of capabilities such as screen sharing, recording, chat, and collaboration tools. Boithok is user-friendly and accessible, with a basic UI that works on both

desktop and mobile platforms. The app's goal is to create a safe and dependable platform for virtual meetings and events, particularly for Bangladeshi enterprises and organizations. Boithok is accessible in both free and paid editions, with pricing based on the number of attendees and meeting duration.

19. **SSL/TLS Support in Government Websites (https):** To improve security and secure user data, the Bangladesh government has made efforts to boost the usage of SSL/TLS support (https) in its websites. The government announced the Secure Government Network (SGN) program in 2017, which mandates that all government websites be housed on secure servers that use SSL/TLS encryption. This effort also includes training sessions for government information technology employees to improve their knowledge and skills in implementing SSL/TLS security measures. By 2021, the majority of government websites in Bangladesh, including those for the Prime Minister's Office, the Ministry of Finance, and the Bangladesh Police, have implemented SSL/TLS encryption. Nonetheless, certain government websites continue to lack SSL/TLS support, posing security hazards to consumers. To guarantee internet users' safety and privacy, the government continues to advocate the adoption of SSL/TLS encryption on all official websites.

The Digital Bangladesh inventiveness includes:

- (i) developing human resources for the twenty-first century,
- (ii) connecting citizens in ways that are meaningful to them,
- (iii) bringing services to citizens' doorsteps, and
- (iv) using digital technology to make the private sector and market more productive and competitive.

### **5.5.2 Leveraging 4IR to achieve knowledge-based economy**

Bangladesh is preparing for the Fourth Industrial Revolution (4IR). Rarely a day goes by without a national political leader or a significant civil society figure bringing up 4IR issues in the national media. 4IR may possibly be considered the country's new buzzword. As upon joining this big worldwide movement, the country face numerous

obstacles and opportunities that, if handled correctly, might lead to significant transformation, growth, and progress.

A crucial part of accomplishing the SDGs is technology. Undoubtedly, ICT serves as a catalyst for more effective resource management, education, and business operations—all of which are crucial success factors for achieving the SDGs. Technology, especially the digital technology stack powering 4IR, which consists of more than a dozen cutting-edge innovations ranging from artificial intelligence to block chain, has the potential to enhance resource utilization, service delivery, progress monitoring, and the formation of cooperative alliances. The skills needed to complete tasks will continue to evolve as task content development transitions. Skill demand is influenced not just by the degree of automation, but also by the products produced by businesses, industries, and the country. In addition to automating existing processes, the 4IR technology stack allows for the introduction of new ones, such as remote service delivery.

### **5.5.3 Moving from factor-based stage to Information-based economy**

Bangladesh faces a significant challenge in forming an innovation economy so that its economic growth from TFP contributions continues to improve from 0.3 percent to 4.5 percent by 2041. A three-pronged approach will be required:

- i. Software and process innovation, as well as service digitization.
- ii. Combining labor advantage with science and high-tech innovation; and
- iii. Taking use of the fourth industrial revolution - artificial intelligence and smart machines - for competitiveness and a low-carbon economy.

Furthermore, the government must progressively move its focus away from direct service delivery and toward the creation of enabling digital platforms and infrastructure that allow the private sector, civil society, and academics to collaborate and meet citizens' needs for modern tailored services.

### **5.5.4 Building Transport and Communications Infrastructure for sustained growth**

Investing in transportation and communications infrastructure to ensure long-term growth, low-cost, efficient transportation is a crucial determinant of the economy's competitiveness in today's globalized economy, influencing trade and investment flows both internally and externally. As a result, developing an efficient and low-cost



transportation network is a critical factor of the ability to meet growth and poverty targets.

Finally, all government agencies will improve service delivery simplification and embrace innovation and digitization through an organized, multi-stakeholder engagement process that can expedite procurement, capacity development, implementation, maintenance, and upgrades in order to achieve the information society. In this case, data is critical for assessing development progress, planning development initiatives, and reducing social exclusion. As a result, it will be critical to take advantage of the emerging data revolution to assure evidence-based policymaking in order to accelerate progress, improve existing services, and create new ones.

Simultaneously, to ensure that economic progress is sustained, and social cohesiveness is strengthened, the potentially powerful negative side effects of technology must be addressed proactively, continuously, and adequately. Alarming trends like the spread of fake news and megacorporation's ownership of personal data must be tackled by citizen-centric regulation and widespread digital literacy.

Artificial intelligence, robotics, quantum computing, and 3D printing are disrupting industries as diverse as agriculture, manufacturing, and healthcare. Robotics and automation, among other technologies, will have a big impact on jobs and the future of work. The problem is figuring out how to use transformative technology to create more jobs than that are going to be destroyed because of technological advancement.

## CHAPTER VI: ANALYSIS AND FINDINGS

### 6.1 Overview

The persistence of data analysis was summing up of collected data for simpler understanding and equipping responses to the research question (Yaokumah, 2013). For this paper, the research questions were- (i) Which are the major threats evolving in government Critical Information Infrastructures (CII) and how do they affect the organizations; (ii) What are the significant security measures adopted to protect sensitive government information; and (iii) How those threats could be minimized in public information domain? The Null Hypothesis ( $H_0$ ) was- Existing practicing security system is not good enough for protecting government critical information infrastructures and the Alternative Hypothesis ( $H_1$ )- Existing security system is sufficient for protecting government critical information infrastructures.

Bangladesh is rapidly developing in the IT sector. Dhaka, which is the capital of Bangladesh, is establishing itself as a freelance IT and IT-enabled services outsourcing (ITES) hub. Though it has yet to make a significant contribution to the nationwide economic system, it is a significant growth sector and expected to grow further. Since 2009, the country's Information and Communications Technology (ICT) industry has averaged 57.21% economic growth. Over the period of recent years, significant progress has been made in the IT sector toward creation of a "Digital Bangladesh," with additional efforts on the way. Even though the IT and outsourcing sectors are booming in the country, the lack of universal broadband internet access and the high cost of interconnection remain impediments to the IT industry's expansion. To help Bangladesh's IT industry, the government has launched on a few large-scale information and communication technologies (ICT) initiatives with a long-term perspective.

This research solely focuses on government organizations, though information security is a concept that has significant effect for both government and non-government organizations. In this study, 04 (four) important Bangladesh government organizations were taken into consideration. Each of them incorporates and works with large scale IT infrastructure and they play specific roles which are quite different from each other, having separate organograms and their controlling ministries were

also not similar. Following subsections represents the fundamental knowledge on the selected institutions- what are they, how they function, application of Information Security on the activities of the selected Bangladesh government organizations-

## **6.2 Identity of Studied Organizations**

With the rapid digitalization of the government infrastructures, currently most of the government organizations incorporate the Information Technological aspects. This chapter briefly introduces the four crucial organizations that has been studied in this research work and it also includes their roles - how important they are and application of information technology in their day-to-day activities.

### **6.2.1 Bangladesh Bank-**

The Bangladesh Bank (BB) is the country's main bank and the country's financial governing body. It is based in Dhaka and was established under the Bangladesh Bank Order, 1972 (P.O. No. 127 of 1972), which took effect on December 16, 1971. The bank is a founding member of the Micro Finance Partnership and is actively pursuing green banking and financial inclusion programs.

The Bangladeshi government controls the whole central bank, which is responsible for regulating the country's economic and budgetary policies. Bangladesh Bank is the first central bank in the world to set up a dedicated helpline (16236) for clients to report any banking-related difficulties. In addition, the bank is the first central bank in the world to implement a "Green Banking Policy."

Bangladesh Bank is the banking entity with sole responsibility to provide the government with currency as a central bank, reserve bank, or monetary authority. Bangladesh Bank is the banking entity with sole responsibility to provide the government with currency as a central bank, reserve bank, or monetary authority. As a 'lender of last resort,' Bangladesh Bank, like any other commercial bank, charges interest on loans made to customers, primarily governments and other commercial banks. A central bank, on the other hand, differs from a standard commercial bank in that it has the copyright to create currency, which is subsequently leased to the government as legal tender. It is a bank that can lend money to other banks in times of need. Its primary job is to keep the country's economy growing, but it also has more

active responsibilities including controlling reduced interest rates and acting as a last-resort borrower for the banking industry during times of economic crises (private banks often being integral to the national financial system). Bangladesh Bank, as a central bank, has administrative powers to ensure that banks and other financial institutions do not engage in dangerous or unlawful activities. The Bangladesh Bank conducts all of the responsibilities that a banking system is supposed to do in any country like managing market stability via economic and financial measures, maintaining the country's foreign currency and gold reserves, and supervising the banking sector etc.

The Bangladesh Bank's (BB) aim is to act as a modernized, innovative, efficient, and forward-looking banking system, managing the country's monetary and financial system with the aim of implementing an internally and externally value of Bangladeshi Taka conducive to rapid economic progress and prosperity. To accomplish the goals, the Bangladesh Bank (BB) primarily i) conducts monetary policy and (ii) supervises banking and non-banking financial institutions (NBFIs) in order to create a strong financial system. As Bangladesh's central bank, BB conducts all of the following typical functions of a central bank around the world.

- (1) In the best national interest, BB formulates and implements monetary policy aimed at stabilizing internal financial value and maintaining competitive external per worth of the taka.
- (2) In the domestic capital market and foreign exchange market, BB formulates and implements intervention policies.
- (3) In order to promote the banking system's security, integrity, and sustainability, defend depositors' interests, and maintain trust in the banking system, the BB supervises, and controls planned banks and non-bank financial institutions (NBFIs), including off-site and on-site monitoring.
- (4) The global reserve, which comprises BB's gold, foreign exchange SDR, and IMF reserve position, is completely the responsibility of BB.
- (5) The Bangladesh Bank has sole authority to issue bank notes as the country's central bank.

(6) The Bangladesh Bank acts as a clearing house for planned banking institutions to clear and settle inter-bank payments arising from the exchange of cheques, drafts, bills, and other similar instruments.

(7) The Bangladesh Bank acts as a banker to the government.

(8) The Bangladesh Bank acts as a lender of last resort for the government and the country's scheduled ban.

"It offers the Government of Bangladesh with functional and advisory services on topics pertaining to the Government's debt management policy and the issuing of various treasury instruments," according to the BB Order-1972. BB's Debt Management Department (DMD) is also in charge of overseeing and regulating the principal dealer (PD) system, as well as creating the main and secondary markets for government securities (G-Sec)."

According to their website (<https://www.bb.org.bd/en>), The Bangladesh Bank incorporates an e-Recruitment system (<https://erecruitment.bb.org.bd/>) and offers various online services that requires a strong IT infrastructure and a decent amount of IT security to ensure a safe and secure online environment. Some of the services include:

- CIB services: The automated CIB service provides credit-related information to prospective and existing borrowers in order to foster a disciplined borrowing environment. Risk management will be more effective with this improved and efficient system. Banks and financial institutions can provide credit information to the CIB database 24 hours a day, seven days a week, and they can access credit reports from the CIB online.
- Agent Information Management System: The Authorized Dealer Bank will use this system to transmit the relevant information and documentation in order to grant authorization to serve as a local agent for a foreign principal under Section-18A of the Foreign Exchange Regulation Act of 1947.
- goAML reporting: GoAML refers to the UNODC's response to money laundering. The goAML Client application is a system for intelligence analysis created for use by the Bangladesh Financial Intelligence Unit (BFIU), the primary organization in Bangladesh tasked with analyzing Suspicious

Transaction Reports (STRs), Cash Transaction Reports (CTRs), and information related to money laundering (ML)/terrorism financing (TF) obtained from reporting organizations and other sources, as well as disseminating information/intelligence to pertinent law enforcement agencies. The goAML Web application offers a secure web-based interface for sharing stakeholder information, filling out online report forms, sending XML files as attachments by secure e-mail, and uploading electronic reports such as XML files between the BFIU and its reporting companies.

- **Web Upload:** All scheduled banks are required to submit a Weekly Statement of Position to the Department of Off-site Supervision every Thursday at the close of business, according to Article 36(3) of the Bangladesh Bank Order, 1972. Within three (3) working days after the reporting date, this statement must be filed electronically utilizing this web service.
- **System for Monitoring and Managing Foreign Exchange Transactions:** Bangladesh's total foreign exchange transactions are monitored using the Online Foreign Exchange Transaction Monitoring and Management System. Export, Import, Inward remittance (Wage Earners' remittance and other) and Outward remittance are all part of the system (Traveling and Miscellaneous). Banks and AD Branches use its services to issue and report Foreign Exchange Transactions to Bangladesh Bank.
- **Banking Information on Mobile Apps:** In Bangladesh, a mobile app for ATM Booths and Branches location details, as well as services provided to customers, is available.
- **e-Tendering System of the Bangladesh Bank:** To aid in the procurement process, Bangladesh Bank introduces an online tendering system. You can use the system to participate in Bangladesh Bank's local and international tenders and procurements.
- **e>Returns:** An online portal (<https://etaxnbr.gov.bd/>) that allows Scheduled Banks and Non-bank Financial Institutions (NBFIs) to submit Electronic Returns via respective BB Departments using a specified template for Macro Economy Analysis. Another online portal service provided by Bangladesh Bank's Statistics Department allows Other Financial Corporations (OFCs) to

submit electronic returns using predefined templates (RIT) for macroeconomic research

- System for "Special Foreign Currency Account Monitoring (SFCAMS)": Bangladesh's FC account transactions are monitored using the Online Special Foreign Currency Account Monitoring System. AD Branches of Banks report day-to-day Transactions (Only Special FC A/C) to BB via its services.
- "Information for Deposit Insurance Premium Assessment (IDIPA)": The Deposit Insurance System (DIS) is now helping to maintain financial stability by safeguarding bank depositors and ensuring insurance benefits in the unlikely event of a Scheduled Bank failure. The fundamental objectives of DIS are to retain public trust and to increase savings to boost the financial sector's resilience. DIS is now operated by '*The Bank Amanat Bima Ain, 2000*' in Bangladesh.
- "Corporate Memory Management Systems (CMMS)": Corporate Memory Management Systems is a web-based application that monitors Schedule Commercial Banks/FIs and their executives for errors, omissions, and violations of regulations and policies.
- CRR and SLR e-statements: All scheduled banks in Bangladesh (including conventional and Islamic banking) are required to disclose Thursday positions of demand and time liabilities for the computation of CRR and SLR at the close of business, according to Article 36 of the Bangladesh Bank Order, 1972 and the Bank Company Ain, 1991. By the 10th of the following month, this statement must be sent electronically to the Department of Off-Site Supervision (DOS) via this web service.

Bangladesh Bank offers a wide range of online services and to make sure the system is up and running ensuring the security of the whole system the Bangladesh Bank has a dedicated "ICT Infrastructure Maintenance and Management Department". The purpose of this department is to ensure that automated ICT services run smoothly. The department is in responsible of providing BB users with high-quality ICT assistance. ICTIMMD is also in charge of the technological implementation of a good number of critical national-level operations, including Real-time Gross Settlement (RTGS), Bangladesh Automated Clearing House (BACH), National Payment Switch (NPS),

and CIB online, as well as the Foreign Exchange Transaction Monitoring System (FXTMS). In addition, the department supervises creating and maintaining BB's ICT security policies, as well as guidelines for banks and non-bank financial companies (NBFIs). It audits and inspects BB's ICT infrastructure-related activities, as well as those of all other banks and NBFIs. In addition, the department gathers information on fraudulent practices and security threats (from a variety of banks and financial organizations) and assists in the deployment of suitable countermeasures to avoid such destructive acts. The agency collaborates on Cyber Security concerns with the Ministry of Posts, Telecommunications, and Information Technology's ICT Division, as well as the Bangladesh Computer Council (BCC). It also helps government and non-profit organizations automate their processes. The next Organizational IT Setup chapter will go through the details of this department and its wings.

### **6.2.2 Election Commission-**

Election Commission (EC) Bangladesh is a constitutional organization. It has been functioning freely to hold different types of elections on a regular basis with highest transparency and accountability. It issues election dates, defines communities, compiles electoral rolls, monitors elections, releases results of the election, and appoints election tribunals to resolve election disputes. The EC has a major role for strengthening democracy through holding free, fair and impartial election which paves the way for launching good governance inside the country.

The Commission also performs other accomplishments which are associated with election management such as the supervision of polling stations, election schedules declaration, control of officials during the election, promoting public awareness regarding voting rights and preparation, announcing and publication of election results. EC confirms right solicitation of laws by resolute of election disagreements and grievances as well.

The Election Commission is theoretically obligated to oversee free and fair elections for the presidency, the *Jatiya Sangsad*, and local government organizations. All major parties retain close contacts with the Election Commission. All political parties are invited to participate in discussions about the election schedule, election process, and general election procedures. With competing political parties, discussions are held on topics such as voter registration, the compilation and modification of electoral rolls,



and other related topics. When the Election Commission has more than one member, the Chief Election Commissioner serves as chairman. The duration of service for any Election Commissioner is five years from the date he takes office, according to the Law. A member who has served as Chief Election Commissioner is ineligible for nomination to the Republic's service. Any other Election Commissioner who resigns from that position is eligible for appointment as Chief Election Commissioner, but not for employment in the service of the Republic. The Bangladesh Election Commission now consists of three members, one of whom is the Chief Election Commissioner. The Commission may allocate to its chairman, any of its members, or any of its officers all or any of its legal authorities and duties. The Commission could demand any person or authority to undertake such activities or provide such support for the purpose of investigation as it sees fit.

"Digital Bangladesh" embraces modern technology to establish democracy, human rights, transparency, accountability, and justice, as well as to ensure citizens' access to government services. It is an all-encompassing vision that promotes human resource development, community involvement, civil services, and the use of information technology in business. The Bangladesh Election Commission (BEC) is now trying to build a complete National Identification (NID) system based on the voter database, keeping this aim in mind. This will, among other things, improve the State's ability to integrate the use of ICT to safeguard people' identities, compile data, prevent leakage, promote inclusion, and improve data management reliability and efficiency. BEC manages NID as part of the Identification System for Enhancing Access to Services (IDEA) initiative, which is funded by the World Bank. In Bangladesh, electronic voting machines (EVMs) were introduced by the Election Commission to address issues with paper ballots and to pave the digitalization in the electoral system of Bangladesh. They were initially successfully employed in 2007 for the election of the Dhaka Officers' Club's working committee. EVMs have been utilized sparingly in several city corporation elections throughout the country since then. The majority of Bangladeshis reside in rural areas. They are uninitiated in the use of new voting tools. It's also a way that informed voters are utterly unaware of. As a result, the Election Commission has dispatched expert trainers to various parts of the country to educate voters on the norms and regulations of voting using electronic voting machines. Also, with the progress in the voting system, there are some concerns also for which the

commission is continuously working in order to address those concerns and make sure that the electoral process is up and running.

In carrying out its duties, the Election Commission is an independent government institution bound only by the Republic and any other law. The commission can persuade any individual or authority to fulfill such duties or provide such services as it considers necessary for the election process. Preparation of correct polling roll, preparation and circulation of National Identity Cards and conducting free and fair elections according to true voting rolls is the main responsibility of the EC, Bangladesh. The commission has to undertake critical and crucial roles and responsibilities which requires a strong IT infrastructure. So, making sure that it is secure is a topmost priority for the government.

### **6.2.3 Bangladesh Police-**

Bangladesh Police is the state Police Organization of Bangladesh. The civil force is extended all over the country and it serves a critical role in keeping peace and enforcing the rule of law in Bangladesh. Bangladesh police performs under the administrative mechanism of the Ministry of Home Affairs (MoHA), Bangladesh. Police are the most visible part of the law & order enforcement agency and very concerning section of the criminal justice system. However, the police are mainly responsible for maintaining law and order as well as the safety of individuals and their property, they also play a significant part in the criminal justice system.

Bangladesh Police is the country's primary law enforcing agency. It is controlled by the Bangladeshi government's Ministry of Home Affairs. It is the most important and vital part of preserving the state's law and order. Though the police are mainly engaged with maintenance of law and order and ensuring the safety of people and property, they also have other responsibilities. Bangladesh's formal and structured police, which includes a wide range of operations, has evolved and developed over a lengthy period to reach this point.

Role of police is very noteworthy to control crime inside the country. Public security and safety also depend on them. To prevent crime, both proactive and reactive strategy they follow. They are supposed to rescue victim, investigate crime scene,

apprehend suspects, make further investigation, and produce charge sheet or final report. They must encounter with criminals and face with modern criminality. Undoubtedly it could be said that police have a lot of responsibility to establish a peaceful and secure society.

Bangladesh police is organized into ten branches, each with its own way of operation. The Inspector General of Police oversees these divisions, but they operate largely freely. For the training of constables, there are four regional training schools. District police, CID police, Special Branch, Railway police, Traffic police, River police, City police, Cavalier police, Armed police battalions, and Ranges reserves force are the different branches of the police force. Bangladesh Police's origins and legacy are distinguished by a fusion of colonization qualities with a traditional culture's internal security system. The British regime's policing mentality was never compatible with democracy values and political growth. It is critical to the maintenance of calm and the execution of law and order inside Bangladesh. However, the police are mainly focused with the protection of law and order as well as the safety of individuals' people and property, they also play an important role in the criminal justice system. During Bangladesh's liberation struggle, the police played a crucial part.

Bangladesh police is bound to provide safety and security to all the citizen of Bangladesh in every aspect of current time. With the rapid advancement in technology, the lifestyle of the people is becoming more and more tech centric, online oriented. So, challenges like cyber bullying, cybercrimes can go out of hand if not handled timely and correctly. The Cyber Police Center (CPC) is the most recent addition to Criminal Investigation Departments of the Bangladesh Police decades of training excellence. It was built under the Korean International Co-operation Agency's (KOICA)-funded project "Enhancing the Cyber Investigation Capability of Bangladesh Police" and designed by Korean cyber experts. On January 23, 2017, the Honorable Prime Minister and the Ambassador of the Republic of Korea opened the CPC. CPC, along with Detective Training School (DTS) and Forensic Training Institute, has become another flagship for CID, equipped with cutting-edge training amenities, faculties, lodging, and rooftop dining facilities (FTI). It is solely dedicated to cybercrime, cyber security, social media monitoring, and digital forensics training. It has so far produced a pool of over 600 highly skilled officers in the core areas of expertise. CPC is working with the goal of creating a safe and secure digital

Bangladesh by developing human resources that can ensure a safe cyberspace for all Bangladeshi citizens - men, women, and children alike.

The CT-Cyber Crime Investigation, formerly known as the Cyber Security & Crime Division, is a division of Counter Terrorism and Transnational Crime operated by the Dhaka Metropolitan Police of Bangladesh Police. This division's primary mission is to combat terrorism in cyberspace. It also patrols the Dhaka Metropolitan area, preventing, detecting, and investigating cyber-terrorism and cyber-crime.

Police Cyber Support for Women is an all-women cyber support service provided by Police Headquarters in Bangladesh. Dr. Benazir Ahmed, BPM (BAR), Inspector General of Police, launched this service on November 16, 2020. Police Cyber Support for Women assists women in pursuing legal action for cybercrimes committed against them. It provides women victims of cybercrime with the necessary technological assistance. It promotes and disseminates cyber security awareness since its inception. While supporting, Police Cyber Support for women maintain the confidentiality of the victim's information. Its mission is to foster a technologically oriented environment for women in cyberspace. and mission is to provide necessary legal and technological assistance to female cyberspace victims exclusively, as well as to raise cybersecurity awareness.

The increasing number of complaints suggests that women are more comfortable seeking assistance from female officers. As the first responder, PCSW provides victims with the necessary advice and legal assistance, depending on their needs. When necessary, female officers provide necessary counseling to cyber victims. PCSW connects victims to a nearby police station, appropriate police unit, or victim support center for legal assistance and coordinates the investigation procedure.

Bangladesh police, the single most important organization charged with maintaining law and order and human rights, is at a crossroads, deciding whether to accept the position of service rather than force, dedicated to making sure delivery of services, flexibility in responding to society wishes, and social equity. The Special Branch (SB) of Bangladesh Police was established to assist in upholding National security and executes the functions of intelligence and counterintelligence. Community policing is

an organization that promotes community, government, and police collaborations, proactive problem solving, and community participation to tackle the sources of violence, fear of crime, and local issues in Bangladesh police. Bangladesh Police have been attempting to establish this ideology throughout the country. The Police Reform Program (PRP), a UNDP-funded initiative, has been providing technical assistance to Bangladesh Police in order to introduce community policing across the country.

The strategic alliance includes the following:

1. a National Community Policing Advisory Committee directed by the Minister of Home Affairs' Secretary.
2. a National Community Policing Coordination Committee directed by the IGP or a second Inspector General of Police at Police Headquarters.
3. a Crime Prevention Centre established in the police headquarters, with the Detective Inspector General (Crime) as its focal point.

So, from the above representation of the workloads that the Bangladesh Police goes through in order to maintain law and order all over the country, one can easily imagine the requirement of a strong tech centric system and the need of security for the system.

#### **6.2.4 Land Records and Survey Department-**

Under direct supervision of the Ministry of Land the Land Records and Survey Department (DLRC) determine land ownership rights and create Record of Rights (RoR) and Maps. Land ownership of human beings was recorded in *parcha* or say it *shwattalipi*. The Land Record and Survey Department (LRSD) is a government sector in Bangladesh that is in charge of measuring and preserving land records. It is situated in Dhaka, Bangladesh, in the Tejgaon Thana region.

The land is the absolute and most desired wealth of human beings. People love to be owner of land as their life. So, for a country and nation, proper land management is most important thing. Land surveying and the creation of land registry began in full at the turn of the 20th century, region by region. The district-level services were primarily focused on raising revenue. Apart from Chittagong hill tracts (which were populated largely by tribal people) in the northwestern tract of old Bengal, these

efforts, known as surveying and resettlement activities, have been accomplished throughout the entire undivided province of Bengal.

Directorate of Land Records and Survey make surveys of every plot of land of village and make maps at the same time create RoR (*Khatian*). This land management is ongoing process now. Digital methods of land survey were kicked off. Land sketch and *Khatian* print through online system, and database creation is underway performing.

The government plans to automate all land-related services through 18 integrated applications, according to United News Bangladesh, in an effort to make the aging system more dynamic, transparent, and user-friendly. The projected land automation management will produce an interoperable land database that will enable fast and easy online services across the country, including *Namjari*, land development tax, and Porcha collection. There have been three initiatives in this area thus far. The following are the projects: National Land Zoning, Digital Land Record, Survey and Maintenance, and Governance Management (Component B: Digital Land Management System). In addition, Mouza and plot-based national digital land zoning will be implemented to conserve arable land and maintain food security. Following the completion of digital zoning based on land use, choices about protecting and maximizing agricultural land in the country will be possible. In order to speed case resolution and alleviate public suffering, the government has taken steps to unify all revenue court cases into a single integrated networking system. The project, dubbed "Land Management Automation," was approved by the National Economic Council's Executive Committee and is estimated to cost Tk 1,197.0318 crore. According to the officials, after the project is completed, people will be able to make land mutation, lease, and tax payments online without difficulty, in addition to increased transparency in revenue collection. People will be able to access services through 5,247 land offices that will be linked to the internet. When the project is fully implemented, the number of land-related disputes and other incidents will be significantly reduced. It would also lessen the role of middlemen in land-related disputes. The ministry of land will carry out the national digital land-zoning project based on mouzas and plots.

Across the country's 64 districts, the project will span 56,348 mouzas in 4,562 unions of 493 upazilas. Satellite photos and digitalized mouza maps will be used for this digital land-zoning. According to the project proposal, it will handle the collection, scanning, digitization, database building, altering plot checking, geo-referencing mouza map, mouza map matching, and field checking of approximately 1,38,412 sheets of maps. In most countries, a single office handles all land-related services, including land records and registrations. Three offices in Bangladesh, on the other hand, provide services that cause people to suffer and waste time. In land management and registration offices, the present form of land recording follows the time-honored tradition of handwritten paperwork. Bangladesh's land has been divided based on permits, which is still a concern. Surveying and recording are handled by the land ministry, whereas registration is handled by the legal ministry. Bangladesh has a total land surface area of 12.31 million hectares, of which 7.85 million hectares are now used for agricultural, according to the National Land Zoning Project. On the land surface area, around 152.25 million people live. As a result of population expansion, the share of land per capita is shrinking every year, making agriculture, forests, and wetlands more susceptible and disadvantaged. In 1983-84, there were 20 million acres of total cultivable land, but by 1997, that number had reduced to 17.5 million acres. The main factors motivating people in Bangladesh to overexploit natural resources include poverty, fast population increase, poor land use, and ineffective execution of current rules and regulations. Competition for various uses of land resources, massive population expansion, natural and man-made risks, economic opportunities, and ecological hotspots need the creation of "Land Use Based Zoning" in the country to ensure differentiated and sustainable land management systems. The government has acknowledged the importance of this step, according to an official document, and has produced further policies, strategies, and planning papers that expressly address diverse land issues and their integrated management.

Many of the handwritten paper records and registers at land record and registration offices are over a century old, humidified and practically unusable, or half-eaten by booklice, wood worms, termites, mice, and cockroaches. The necessary civil engineering, as well as the necessary equipment, for the construction of a central data center in the Land Record and Survey Department has been completed. A data backup and recovery center has been constructed at the University Grants Commission

(UGC) in the city's Agargaon neighborhood, under the direction of the Bangladesh Computer Council (BCC). Once the system is fully automated, landowners and buyers will not need to visit more than ten government agencies for documentation. All documents will be uploaded to a centralized database, which will be accessible to government authorities and, in some situations, the broader public.

All these government organizations are very important in nature. They generate, process, circulate and archive lots of sensitive classified and unclassified document on daily basis. This information highly influences local economy, politics, and social life even on individuals.

### **6.3 Interview Analysis**

Government of Bangladesh plans to implement Digital Bangladesh in full-fledged. The aim of DLRC is to improve the government service delivery process and to boost the efficiency of the government. With a view to achieve this objective, it is necessary to digitize the critical information, process and stack those digitized information in a way so that the information doesn't get lost or compromised.

The ways and means learned from the interviews of IT personnel have been used in this discussion with the related responses. Diverse achievement features were extracted from the outcomes. An empirical analysis, using a self-administered questionnaire, has been conducted to explore and assess the existing status of ISG of the Bangladesh government organization. The researchers are confident that the collected responses are good enough for analysis and appropriate to attain the objectives of this empirical study.

#### **6.3.1 Present Situation of ISMS and Governance Structure**

Security and privacy concerns exist in every technology-driven corporate operation. Information security is managed by an information security management system (ISMS), which is a set of policies and procedures that maintains safety and hazards comprehensively and throughout your entire organization. It will enable businesses in identifying and addressing risks and possibilities that may exist in relation to your important information and any associated resources. Risk analysis and risk



management are typically the emphasis of ISMS frameworks. Considering it a methodical technique to balancing risk reduction with the cost (risk) of doing so.

The gap study between security and its urgency in the public organizations is mostly troublesome. Security policy is normally a high-level document, labelling the security objectives of the organization and expecting to achieve. The policy text is thus a sign of organization's commitment towards information security and due persistence. At the same time IT staffs to implement controls and pledge procedures for achieving the specified security goals. The task of breaking up the high-level security policy into actionable, implementable components is then the obligation at the middle-level staffs.

Recently, most of the public agencies of Bangladesh have been brought under the e-governance framework. Different government Ministries/Divisions, Departments/agencies and their subordinate bodies have been incorporated in bangladesh.gov.bd portal. This web portal contains several thousands of government organizations websites and considered the largest domain of its kind.

Bangla daily the *Prothom Alo* quoted ICT state minister as on 25/6/2021, he was addressing a virtual program and comment that "The government is working to make all citizen services available online in the coming four years". The state minister further added, the payment system has been digitized, which has led to rapid growth of mobile financial services and e-commerce.

The questionnaire for ISMS survey was conducted from May to mid-August 2021 in four important state-owned organizations with a view to achieve better understand on the current situation of Information Security program and governance structures. The 19 interview questions (Annexure-I) incorporated the following broad areas-

- a. Organizational IT setup.
- b. Information Security Incidents associated threats and its consequence.
- c. Preventive technologies; and
- d. Safeguarding and Reactive measures to the incidents.

Following is the transcribe of data received from the several Government organizations-

### **6.3.1.1 Organizational IT Setup-**

Bangladesh Bank (BB) has its own IT cell and stores all banking and operational data in 4 tier data center of ICT division. BB has at least 250 employees worked at IT cell. The central bank started its IT securitization process since 2000. Bangladesh Bank has crafted 'Guideline on ICT security for Banks and non-Bank Financial Institutions, May-2015'. It is basically based on Bangladesh Government's Information Security Policy Guidelines and ISO 27001 (Nasser, 2017). The central bank has a well-structured organogram. One deputy governor has been responsible to look after the IT cell. IT cell initially report to the Deputy Governor for any kind of IT incident. The ICT Infrastructure Maintenance and Management Department (ICTIMMD) was established to help Bangladesh Bank (BB) maintain a stable IT atmosphere. The goal of this unit is to guarantee that automatic ICT services run smoothly. The division is in charge of providing high-quality ICT assistance to BB customers. In addition, the agency is responsible for designing and monitoring ICT security measures for banks and non-bank financial institutions (NBFIs). It supervises and inspects BB's, as well as all other banking and NBFIs', ICT infrastructure-related activities. Furthermore, the department gathers information on deceptive practices and security risks (from a variety of banks and financial organizations) and assists in the implementation of suitable countermeasures to avoid such criminal activity. For Cyber Security problems, the agency collaborates with the ICT Division of the Ministry of Posts, Telecommunications, and Information Technology, as well as the Bangladesh Computer Council (BCC). It also works with government and non-profit organizations to automate their operations.

The operations of the organization have been separated into 8 different wings:

1. Wing of Crucial Operation Management
2. Management and Maintenance of Servers and Storage wing
3. Management and Maintenance of the Network wing
4. Management and Maintenance of End User Devices and Helpdesks wing
5. Monitoring and Control of ICT Infrastructure and Emergency Response wing

6. Wing of ICT General Services (Hardware and Infrastructure)

7. Infrastructure Regulatory Compliance Division wing

8. Inventory and Disposal of ICT Hardware Wing

In July 2019, Bangladesh Bank established a Cyber Security Unit (CSU). The activities of the said unit began in May 2020, with the appointment of Md. Mehedi Hasan as the head of the CSU, Bangladesh Bank, by the Chief Information Security Officer (CISO). CSU's functions include:

a. designing and implementing, directing the completion of BB's ongoing cyber security strengthening program and carrying out annual reviews thereof to identify, access, and coordinate remediation of weaknesses in BB's IT security systems. BB's information security infrastructure to monitor IT installations and systems for unauthorized access and use.

b. Implement suitable documented processes, procedures, and internal technical controls in the fields of security engineering (SE), security threat and vulnerability management (STVM), information security operations center (ISOC), security information and event management (SIEM), critical incident response team (CIRT) for the entire financial sector (CIRT), and cyber security intelligence (CSI).

c. Assess knowledge/skill enhancement needs for new CSU staff, establish appropriate cyber security capacity building training routines, and maintain an up-to-date understanding of emerging trends in information security technology.

d. Ensure BB's readiness to respond to IT security problems by creating and regularly practicing incident response and procedure templates. You should also build your leadership abilities to get things done in cross-departmental and cross-agency team settings.

e. Encourage and support a culture of cyber security risk awareness among all BB staff members and departments, and make sure that all BB information assets are effectively, efficiently, and protected.

f. Create security standards for the IT platform that adhere to BB's IT architecture, risk profile, and policy requirements.

g. Collaborate with business units and IT stakeholders to identify requirements and evaluate their suitability for BB's IT infrastructure.

h. Find ways to improve the performance and responsiveness of BB's security work programs.

i. Examine and make recommendations on how to set technical requirements in IT equipment/consumables procurements in accordance with BB's information security architecture and risk profile.

j. Create a short- and long-term security policy for BB, as well as an implementation plan.

Take the necessary steps to upgrade and maintain BB's security infrastructure in accordance with the implementation plan.

k. Assist in the organization of regular security testing on BB's ICT infrastructure, audit existing systems, and provide comprehensive risk assessments.

l. Ensure that logs of user activities are reviewed on a regular basis in order to detect suspicious behavior.

m. To create a policy for automatic (machine learning-based) monitoring and financial fraud detection.

n. Create a monitoring plan for the security policy implementation process by Bangladeshi banks and NBFIs.

o. Assist Bangladeshi banks and non-bank financial institutions (NBFIs) in taking appropriate preventive measures in the event of a security threat or incident at any financial institution in Bangladesh or relevant organization abroad.

p. On a regular basis, facilitate a security awareness program for all bank employees.

q. To investigate any incident, gather a team of digital forensic investigators.

Assist in the integration of IT development systems with security policies and information protection strategies.

- r. Establish an IT security risk management program in collaboration with key stakeholders.
- s. Anticipate new security threats and keep up with changing infrastructures.

According to their website (<https://www.bb.org.bd/aboutus/regulationguideline>) Bangladesh Bank has specific guidelines on ICT security for banks and NBFIs. In recent years, the banking industry has changed the way it provides services to customers and processes information. This historic shift has been brought about by ICT. Electronic banking is becoming more popular, which is increasing financial inclusion adoption. As a result, financial institutions' information security has become increasingly important, and it is necessary for us to guarantee that threats are appropriately detected and controlled.

Information and information technology systems are also important assets for banks and non-bank financial institutions, as well as their clients and stakeholders. Banks and non-bank financial firms rely on information assets to provide services to their consumers. The long-term viability of organizations depends on the protection and upkeep of these assets. Banks and non-bank financial institutions (NBFIs) are responsible for protecting data from unauthorized access, change, disclosure, and destruction.

Banks and NBFIs use a risk-based approach to business, which means that ICT risk is related to the financial system and must be managed with thought and effort. The new ICT Security Guideline for Banks and NBFIs from the Bangladesh Bank should be utilized as a basic requirement and tailored to the amount of technology employed in their operations. The controls and procedures that must be developed to protect the security of information and ICT systems are laid forth in this ICT Security Guideline in a logical manner. This policy applies to all electronic information that is generated, received, saved, replicated, printed, scanned, or manually prepared. The contents of this Guideline apply to: a) Banks and NBFIs in relation to all of their information systems. b) All activities and operations necessary to ensure data security, including facility design, physical security, application security, network security, ICT risk management, project management, infrastructure security management, service delivery management, recovery plans and business continuity planning, alternative

transportation supply chain, acquisition and implementation of information systems, hardware and software usage, waste treatment policy, and safeguarding of personal information.

Based on the architecture of its primary business application solution, ICT infrastructure, operational environment, and procedures, a bank or NBFIs can be categorized as follows: Category-1: Centralized ICT Operations for managing core business application solutions via Data Center (DC) with backup assets for critical service continuity, including Disaster Recovery Site (DRS)/Secondary Data Center to which all other offices, branches, and booths are connected via WAN with 24x7 attended operation, including Disaster Recovery Site (DRS)/Secondary Data Center to which all other offices, branches, and booths are connected via WAN with 24x7 attended operation. Decentralized ICT operation for managing distributed business application solutions hosted at DC or operational office spaces with standby equity for the progression of key services linked through WAN or with self-contained processes.

ICT Security Management is responsible for ensuring that ICT services and operations are handled effectively and efficiently. Banks and non-bank financial institutions (NBFIs) must be aware of ICT capabilities and be able to evaluate and appreciate potential abuse opportunities and hazards. They must ensure the proper documentation of systems, particularly those that support financial activities and reporting. They must take part in ICT security planning to guarantee that resources are allocated in accordance with business goals and that sufficient and qualified technical employees are engaged to ensure that the ICT operating area's continuity is not jeopardized.

ICT Security Management includes factors such as roles and responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, and Insurance or Risk Coverage Fund. While properly defined roles and duties of the Board and Senior Management are crucial when establishing ICT Governance, adequately defined roles also allow for effective project control and organizational expectations. The stakeholders in ICT Governance include the Board of Directors, CEO, ICT Steering Committee, ICT Security Committee, CIO, CTO, CISO, Management Committee for Risk, Chief Risk Officer, and Business Executives.

It also includes-

a) Approving ICT strategy and policy documents is one of the Board of Directors' responsibilities.

b) Ensuring that management has put in place an effective project plan.

c) Accepting that the ICT approach has been chosen appropriately.

d) Making sure that the ICT organizational structure supports and guides the business model.

e) Ensuring that ICT stocks are well-balanced in terms of risks and rewards, and that they are kept within reasonable budgets.

f) Verify that the ICT Security Policy is complying.

Obligations of the ICT Steering Committee an ICT Steering Committee with representation from ICT, Risk, HR, ICC/Audit, Legitimate, and other associated Business Units must be formed.

The committee will-

a) keep track of management techniques for establishing and attaining key objectives,

b) understand ICT risks and controls,

c) provide risk, finance, or sourcing recommendations,

d) ensure project priorities and feasibility for ICT proposals,

e) ensure that all key projects include a "project risk management" component,

f) counsel and advise on system planning within rules,

g) ensure that new technology risk assessments are carried out,

h) strictly adhere to regulatory requirements,

i) provide architectural guidance and ensure that ICT architecture reflects the requirement for legislative and regulatory compliance.

Obligations of the ICT Security Committee representatives from the ICT, ICT Security, Risk, ICC, and Business groups must form an ICT Security Commission. It will-

- a) Ensure that ICT security objectives, policies, and procedures are developed and implemented,
- b) Ongoing support from management for information security processes,
- c) Maintain ongoing compliance with ICT security corporate objectives, regulatory, and legal requirements,
- d) Assisting with the development of an ICT risk management framework/process, as well as the establishment of acceptable ICT risk tolerances, risk aptitude, and assurance standards,
- e) On a regular basis, review and approve changes to ICT Security practices.

ICT risk is a part of a company's overall risk profile. Strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, and so on are some of the other hazards that a bank or non-bank financial institution encounters. ICT-related risk is viewed as a component of operational risk by many firms. Even strategic risk, on the other hand, might have an ICT component, especially if ICT is a key enabler of new business measures. The same may be said for credit risk, where a lack of ICT security can lead to poorer credit ratings. It's best not to depict ICT risk as a hierarchical reliance on another risk category.

The risk of business risk associated with the usage, possession, process, involvement, impact, and acceptance of ICT within a bank or NBFI is referred to as ICT risk. It was made up of ICT-related events and circumstances that may or may not have an impact on the company. It can occur at any time and with varying degrees of severity, making it difficult to fulfill strategic goals and objectives. The expression of ICT risks in clear and succinct enterprise aspects is required for meaningful ICT risk assessments and risk-based choices. Risk management involves collaboration between ICT and the business whose risk must be managed.

All decision makers must be able to understand and communicate how bad events may affect business goals. a) An ICT professional must be aware of how ICT-related errors or actions might damage business objectives and result in direct or indirect



losses. b) A business owner must understand how ICT-related failures or incidents affect important systems and functions. The purpose of risk response is to align measured risk with the risk level set by the institution. In other words, a reaction must be designed so that as much future residual risk as possible (typically based on available resources) falls within the risk tolerance. A reaction must be defined whenever the risk assessment reveals risks that are outside of the established tolerance thresholds. Risk avoidance, risk reduction/mitigation, risk sharing/transfer, and risk retention are the four possible reactions.

The following are the BB guidelines for this purpose:

a) The bank or non-bank financial institution (NBFI) must produce a set of risk indicators,

b) Key Risk Indications are most likely to be indicators for business-critical risks,

c) The bank or NBFI must make every effort to implement, measure, and report various equivalent sensitivity indicators,

d) Following risk analysis, the bank or NBFI must define risk response in order to align risk with the bank's or NBFI's defined risk appetite,

e) By implementing proper risk management processes, the bank or NBFI must increase overall ICT risk management practices,

f) The bank or NBFI must put in place a range of control measures targeted at reducing either an adverse occurrence or the event's business impact.

The dynamics of technology operation management, such as capacity management, request management, change management, incident and problem management, and so on, are all addressed by ICT Service Management. The goal is to implement controls that will allow for the greatest degree of ICT service quality while minimizing operational risk. When the routine supply of ICT services is disrupted suddenly, it is called an incident. Such situations must be adequately managed by the Bank or NBFI in order to avoid a situation of mishandling that results in a long-term disruption of ICT facilities.

The bank or NBFI must design an incident management strategy with the goal of restoring normal ICT service as quickly as feasible after the event, with the least

amount of disruption to business operations. The Bank or NBFi must also describe the role of employees who will be involved in the incident management process, which includes recording, analyzing, resolving, and supervising incidents. It is critical that instances are assigned the appropriate severity level. The Bank or NBFi may entrust the purpose of determining and assigning incident severity levels to a technical helpdesk function as aspect of incident analysis. The bank or NBFi must prepare tech support personnel to identify the significant incidents. Furthermore, methods for evaluating the severity of incidents must be established and documented.

The bank or non-bank financial institution shall establish corresponding escalation and resolution guidelines, with resolution timeframes correspond to the severity level of the event. The security incident escalation and response plan must be evaluated on daily basis. The bank or NBFi shall establish an ICT Emergency Response Team comprised of staff from the bank or NBFi who have the necessary technical and operational skills to handle unexpected events. In some cases, major incidents can quickly escalate into an emergency. The status of such occurrences must be reported to top management so that an early decision to activate the disaster recovery plan can be made. In the occasion that a crucial system fails over to its disaster recovery system, the bank or NBFi must notify Bangladesh Bank as quickly as possible. Any major incident must be communicated to customers by the bank or NBFi. The ability to maintain customer confidence during a crisis or extreme case is critical to the bank's or NBFi's prestige and reliability. While the objective of incident management is to immediately restore ICT service, the objective of problem management is to locate and eliminate the root causes in order to prevent recurrent incidents. Capacity management seeks to maintain cost-effectiveness while ensuring that ICT capacity satisfies present and future business requirements.

The ICT landscape is vulnerable to a variety of cyber-attacks. The frequency and severity of such attacks are on the rise. To adequately address related threats, it is critical that a bank or NBFi implements security solutions at the data, application, database, operating systems, and network levels. Appropriate safeguards must be put in place to protect sensitive or confidential information stored and processed in systems, such as customer personal information, account and transaction data. Before accessing online transactions, sensitive personal or account information, customers must be properly authenticated.

Bring Your Own Device (BYOD) is a relatively new practice adopted by banks and financial institutions to allow their staff to access work email, schedules, apps, and information from personal cell devices such as smart phones, tablet devices, and so on. Due to the difficulties in safeguarding, supervising, and controlling employees' personal devices, banks and NBFIs must be aware of the increased potential risks associated with BYOD. Because a bank's or NBFIs critical network infrastructure are concentrated and housed in the Data Center (DC), it is critical that the DC be resilient and physically safeguard from cyberthreats.

The information processing area or Data Center must be physically secure. DC must be a restricted area, with no unauthorized access permitted. Access to DC shall be restricted to authorized personnel only by the bank or NBFIs. The Bank or NBFIs shall only grant DC access on a need-to-have basis. If physical access to the DC is no longer required, it must be revoked immediately. Vendors, service providers, support staff, and cleaning crews must follow strict access authorization procedures. While in the DC, the Bank or NBFIs must ensure that visitors are always accompanied by an authorized employee.

Protection of the Data Center from damage caused by fire, flood, explosion, and other forms of disaster must be designed and implemented. It is discouraged to construct a Data Center and Disaster Recovery Site in a multi-tenant facilitated building. The Data Center layout design, including power supply and network connectivity, must be properly documented. The bank or NBFIs must establish baseline security standards for operating systems, databases, network equipment, and portable devices that comply with the organization's policy. The bank or NBFIs must conduct regular enforcement checks to ensure that the baseline standards are applied consistently and that non-compliances are identified and investigated. A documented plan must be used to implement the Network Design and its security configurations. Different security zones must be defined in the network design.

The primary use of cryptography is to safeguard the integrity and privacy of sensitive or confidential data. Cryptography is widely used in banks and non-bank financial institutions (NBFIs) to safeguard sensitive customer data, including PINs for important apps (e.g., ATMs, payment cards and online financial systems). The secrecy of the key, not the algorithm's secrecy, must be the sole basis for all encryption methods utilized in a cryptographic solution. As a result, the most

important aspect of data encryption is the security and confidentiality of the cryptographic keys used, whether they are master keys, key encrypting keys, or data encrypting keys.

The establishment of appropriate security monitoring systems and processes, the implementation of network surveillance and security monitoring procedures using network security tools, such as intrusion detection and prevention systems, to safeguard the Bank or NBFIs against network intrusion attacks and provide alerts when an intrusion occurs, and their combination are all essential. These measures must be taken to enable prompt detection of unauthorized or malicious activities by internal and external parties. The bank or NBFIs may use security monitoring technologies that track changes to crucial ICT resources including databases, system or data files, and applications to make it easier to spot illegal modifications.

The Bank or NBFIs shall only grant access rights and system privileges in accordance with job responsibility. The bank or NBFIs must ensure that no one, regardless of rank or position, has an inherent right to access confidential data, applications, system resources, or facilities for legitimate purposes.

Disaster Recovery and Business Continuity Management is essential for business resiliency planning in the event of critical catastrophes, operational risks for wide-area disasters, Data Center disasters, and the recovery plan. The fundamental goal of a Business Continuity Plan (BCP) is to enable a bank or non-bank financial institution (NBFIs) to survive a crisis and resume normal business operations. In order to survive with the least amount of financial and reputational damage, a bank or non-bank financial institution (NBFIs) must ensure that vital operations can resume normal processing in a reasonable amount of time. The business resumption and disaster recovery plans must be included in the contingency plan.

The backup, recovery, and restoration processes must all be addressed in the contingency plan. A data backup and recovery policy must be developed by the bank or NBFIs. Each business application must have a backup strategy that is planned, scheduled, and documented, incorporating both on- and off-line backups as well as backup transfer to secure off-site storage. Details of the planned backup schedule for each business application must be created in accordance with the application's categorization and the data it supports, and each point in the backup routine must

define the type of backup needed (full, provisional, gradual, incremental, real-time surveilling).

Any new business function for a bank or a non-bank financial institution (NBFI) requires thorough examination prior to acquisition or development to guarantee that business requirements are met effectively and efficiently. The definition of needs, assessment of alternative sources, review of technological and economic viability, execution of risk and cost-benefit analyses, and conclusion of a final decision to 'make' or 'purchase' are all part of this process. Many systems fail due to insufficient testing and poor system design and implementation. During the system design, production, and validation phases, the Bank or NBFI must detect system flaws and problems. The Bank or NBFI implement a steering committee comprised of business owners, the development/technical team, and other stakeholders to provide oversight and monitoring of the project status, along with deadlines to be noticed at each stage and accomplishments to be met as per the project time schedule. The Bank or NBFI must ensure that activities and processes for developing or acquiring new systems include project risk analysis and categorization, essential success criteria for each project phase, and the defining of project milestones and deliverables when creating a project strategic plan. The duties and activities of project workers must be clearly defined in the project management framework by the bank or NBFI. All ICT projects must have a clearly written and approved project plan. The Bank or NBFI must clearly outline the deliverables to be achieved at each step of the project, as well as the milestones to be met, in the project plans. The Bank or NBFI must guarantee that the relevant business units and ICT management approve user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans, and service performance expectations. The Bank or NBFI will establish project management oversight to ensure that milestones are met, and deliverables are delivered on time. Software documentation must be accessible and securely preserved. All software purchased and installed by the Bank or NBFI must have valid licenses, and a record of the same must be kept by the Bank or NBFI's corresponding unit/department. A separate test environment will be used to undertake end-to-end testing of software functionalities prior to implementation. Before going live, a User Acceptance Test must be completed and signed off on by the necessary business units/departments. The necessary Regulatory Compliance standards for

banking procedures and practices, as well as relevant Bangladeshi laws, must be considered. Any problems or faults discovered as a result of design flaws must be escalated to higher levels within the Software Vendors' organization as well as the Bank/NBFI in a timely manner.

"Channelize through channels" is the new banking paradigm, which relied primarily on the branch network previously. Branchless banking is a distribution channel technique that allows financial services to be delivered without the usage of bank branches. Alternate Delivery Channels are ways to provide financial services to customers directly. Customers can conduct banking activities via ATMs, call the bank's Call Center with any questions, use the digital Interactive Voice Response (IVR), conduct transactions using Internet Banking, and even do transactions on their phones through mobile banking, among other options. These channels have allowed banks to contact a fairly large number of customers regardless of time or place. ADCs improve customer satisfaction while lowering operational and transaction costs. Cardholders have had the facility of withdrawing money and paying premiums to retailers and billing organizations thanks to ATMs and Point-of-Sale (POS) devices. These systems, on the other hand, are targets for card swiping assaults. To ensure that consumers have faith in these systems, the Bank or NBFI should consider implementing the following measures to combat fraudsters' attacks on ATMs and POS terminals:

a) Anti-skimming solutions must be installed on ATM devices by the Bank or NBFI to identify the presence of unknown objects placed over or near a card entry slot,

b) The Bank or NBFI must deploy detection mechanisms and issue notifications to appropriate staff for further investigation and action,

c) To ensure that clients' PINs are transmitted with encryption., the Bank or NBFI must use tamper-resistant keypads,

d) To prevent clients' PINs from being shoulder surfed, the bank or NBFI must take suitable steps,

e) To prevent PIN compromise, the Bank or NBFI may use biometric finger vein scanning technology etc.

Information transmitted over public networks by internet banking facilities must be shielded from unauthorized disclosure or change, dispute, or fraudulent conduct. As financial services are increasingly provided via the internet, banks' internet systems may be vulnerable. As a countermeasure, the bank or NBFBI must develop a security strategy and implement safeguards to ensure the systems' and data's availability, confidentiality, and integrity. The bank or NBFBI must provide assurance to its customers and users that online access and internet transactions are adequately protected and authenticated.

A bank or non-bank financial institution (NBFBI) must carefully assess the security needs related to its online banking system and put in place controls that follow well-known international norms. For all types of online financial transactions, the bank must use 2-FA (two-factor authentication). Tokenization methods based on hardware/software will be preferred. Two-factor authentication's main objectives are to secure the customer authentication process, safeguard the accuracy of customer account information and transactional information, and increase trust in online systems. An online session must be automatically terminated after a set amount of time unless the customer is re-authenticated for the existing session to be maintained.

Payment cards give cardholders the freedom to shop wherever they want, whenever they want. Cardholders can choose to make purchases in person by physically presenting their cards for payment at the merchant, or they can buy online, by mail, or by phone. Payment cards also enable cardholders to withdraw cash from automated teller machines ("ATMs"). Payment cards come in a variety of shapes and sizes, with magnetic stripe cards posing the greatest security risks. Card skimming attacks are possible on sensitive payment card data stored on magnetic stripe cards. Card skimming attacks can occur at any point in the payment card processing chain, including ATMs, payment kiosks, and point-of-sale terminals. The bank or non-bank financial institution that provides payment card services must put in place adequate safeguards to protect sensitive payment card data. The bank or NBFBI must ensure that sensitive card data is encrypted during storage and transmission to ensure the confidentiality and integrity of the data. The bank or NBFBI must ensure that sensitive or confidential information is processed in a secure environment. To manage the risks of working in an unsecured surrounding, mobile transaction controls are required. For operations, the bank or NBFBI must develop security controls, system availability, and

recovery capabilities that are proportionate to the level of risk exposure. External service providers are increasingly being relied on as partners in meeting growth targets and as cost-effective alternatives. ICT outsourcing is available in a range of forms and dimensions. Some of the most popular ICT outsourcing models include systems development and maintenance, support for DC operations, network administration, disaster recovery services, application hosting, and hardware repair. Nowadays, commercial banks outsource various ICT services. Such outsourcing agreements frequently contain performance goals, service levels, availability, dependability, scalability, compliance, audit, security, contingency planning, disaster recovery capabilities, and backup processing facilities. With the introduction of electronic banking, the customer's banking experience is no longer entirely under the control of a bank or NBF. A customer must be ready to conduct secure banking independently in the self-service banking era. It is often said that the greatest way to prevent fraud is for customers to be informed. Increasing consumer knowledge is essential because fraudsters are continuously coming up with new, more intricate scams that access victims' accounts using cutting-edge technology and social engineering techniques. The importance of educating other stakeholders cannot be overstated. Bank employees, who can then act as resources for customer inquiries, law enforcement officials, who can respond to customer complaints with greater understanding, and the media, who can disseminate information accurately and on time, are just a few examples. Users' perception of the relevance and interest of the information is crucial for the effectiveness of awareness campaigns.

The Election Commission has its own IT department where more than 100 staffs are working. Though election commission has its own data server however, it has data backup system host by the data center of Bangladesh Computer Council. This institution started securitization process since 2007. Following the completion of data collection for the electoral roll, the Election Commission intends to establish ICT infrastructure at the Central, District, Upazila, and field data collection team levels to facilitate data collection, verification, and ongoing data management processes, as well as to advance e-governance in Bangladesh through skill development and the sharing/distribution of ICT equipment. Election commission has yet to formulate its own information security policy. They follow national security policy guidelines as



well as best practices in vogue. For any sort of incident, IT personnel report to the system manager. The Guideline's main goals are to:

- a) establish a standard ICT Security Policy and ICT Security Management approach,
- b) assist banks and NBFIs in securing their ICT infrastructure,
- c) create a secure environment for data processing,
- d) establish a holistic approach to ICT Risk Management,
- e) establish a procedure for Business Impact Analysis in conjunction with ICT Risk Management,
- f) Make stakeholders aware of their roles and duties in information security,
- g) Prioritize information and ICT systems, as well as the risks that must be mitigated,
- h) Establish an appropriate project management method for ICT initiatives,
- i) To educate and train users involved in ICT activities in order to achieve business goals,
- j) Establish a system for reviewing the policy on a regular basis,
- k) Ensure best practices (industry standards) in the use of technology, which is not restricted to this guideline,
- l) Assess security risks associated with the usage of Bring-Your-Own-Device (BYOD) and
- m) Minimize security risks associated with electronic banking infrastructure, such as ATM and POS devices, payment cards, internet banking, mobile financial services, and so on.

## Guideline on ICT Security for Banks and NBFIs 2015

Bangladesh Police is working on developing its own infrastructure to combat the new front as cybercrime and terrorism become more common. The government has approved a Tk 1.54 billion initiative to modernize the headquarters' major data center. In order to give better service to the community, Bangladesh Police is gradually introducing cost-effective and long-term information and communication technologies. The ICT sector in Bangladesh is quickly changing. The government of Bangladesh has been pressed to establish and implement national policies and plans to maximize the use of ICT in a socially equitable and just manner, as well as a national goal to achieve the economic position of a middle-income country.

A cost-effective, practical, and long-term ICT strategy and architecture are required as the Police Department gradually modernizes and implements government policy and the reform agenda. PRP will contribute to efforts to promote well-structured and integrated data and knowledge management, as well as information sharing. This objective is meant to support the use of technology in all the other main outcomes. Outcome 6 will first focus on revising and updating the Bangladesh Police Information Management Strategy, as well as developing a costed Master Implementation Plan for the governance, management, procurement, and rollout of the Bangladesh Police ICT Strategy and Enterprise Architecture. PRP will also work with Police Headquarters to build a Police Information Management Division. The ICT focal point for the Police Department will be the Division. This division will be in charge of all areas of ICT system management, governance, and administration. The PRP will provide technical assistance, including training for both specialized and general police ICT professionals and end-users of information management systems. The Bangladesh Police will be able to better manage the resources available to acquire and run cost-effective and long-term ICT with improved capacity. An important input will be the acquisition, implementation, and use of a central police information system for an organization-wide information management data base. The central police information system must be able to adapt to future expansion and evolving technology, as well as support multiple software applications and functions, as well as connection. The ICT system will be gradually implemented at the Metropolitan, Range, and District levels, and finally at each police station, depending

on capital resources and the government's commitment to recurring expenses. The following are regarded to be important outcomes-

- a) ICT Master Plan informs a cost-effective and structured approach to ICT acquisition, installation, and application.
- b) Crime response and prevention improved through better use of information and intelligence.
- c) Community safety enhanced through appropriate application of ICT infrastructure and training.

The police have previously implemented various measures to simplify their services, including the 999-emergency helpline, the Crime Data Management System (CDMS), the Citizen Information Management System (CIMS), Police Clearance Management System (PCMS), Personal Information Management System (PIMS), Integrated Gender based Violence database (PEWR), the IGP Complain Cell, and the BD Police Helpline.

The CDMS promotes productivity in correcting the previously identified issues, and it is a helpful instrument for convenient data analysis, which will enhance the Bangladesh Police's law enforcement activities. It also allows for criminal records checks by Background Check Companies (BCC). The implementation of the CDMS will result in a lower level of threat to Bangladeshi citizens, enhancing nationwide security.

CIMS allows citizens to submit information digitally rather than on paper. It eliminates the need for form printing, distribution, and recollection. Also, by eliminating logistics processing time, you can save time. DMP is a reliable source of information for citizens (Dhaka Metropolitan Police). The citizen can update information about family members and home employees. Apps can also be used to track home change information.

PCMS is an a2i project overseen by the PMO (Prime Minister Office), funded by UNDP, and run by Bangladesh Police. It enables citizens to apply for a police clearance certificate online. There are credit card payment options online, as well as mobile banking options such as bKash. Concerning thana, the authority will verify the

information and print the certificate. At each stage of the process, the applicant will be notified via mobile SMS. After logging into the system, the user can download the completed certificate.

The PIMS project involves the creation of a database of information for approximately 2.25 million police officers. The system's operation is carried out by approximately 1000 units. The Police Information Management System (PIMS) is a decision-making tool for police administration. Every police officer's ID card is generated instantly by the system. Police posting, promotion, training, and joining information is recorded from every unit so that the Head Office has instant access to the information and can make data-driven decisions.

The PEWR project is linked to the CDMS. A good number of Stakeholders will access the database using secured access control via a separate interface. It will be linked to criminals and the prosecution of their cases. The system will generate statistics reports for decision makers, allowing them to take the necessary crime-prevention measures. It is a highly secure Oracle technology-based system that is linked to all units via a secure internet connection via VPN.

This one data center maintains all types of digital information, including the 36 apps created by police to assure efficient and rapid citizen services, which means that when the server goes down, the full suite of digital services is inaccessible. The new data center will contain the intended programs for e-services. The data center project will be implemented by Bangladesh Police, which is part of the Ministry of Home Affairs, from July 2018 to June 2021. The establishment of a centrally managed data center with security, dependability, and tier-III (Tier-III Complainant) for the Bangladesh Police will enhance law and order and advance the socioeconomic growth of the nation. The number of online applications will be increased as part of the project, and existing applications will be upgraded to ensure e-policing. According to project details, Bangladesh Police has decided to upgrade the existing data center to a "State of the Art Data Centre" to host the planned applications for e-services.

It stated that once the project was approved, 42 set computers and accessories would be collected, and 11 software, furniture, and other establishments would have to be developed. The project will boost the quantity of online applications while also modernizing existing apps to ensure e-policing. Situation right now Bangladesh

Police, in keeping with its vision, has already begun office and service automation to increase capacity, provide easy access to police services, deliver better services, and deal with emerging crimes. As mentioned previously, it has developed an ICT Master Plan for the period 2015-2020, computerized most police units, provided ICT training to approximately 30% of officers, and ensured connectivity among all police units. ORP (Organizational Resource Planning) is being developed to improve the management of police assets. Some applications (BD Police Helpline, Hello City, Report 2 RAB) and social media pages are being developed to help citizens file complaints and ask questions. People are given access to various e-services (for example, Online Police Clearance). The Citizen Information Management System (CIMS) software is used to save data relating to the owners and tenants of various residential areas. The Online Crime Data Management System (CDMS) is being kept up to date in order to digitalize and automate police investigations and other investigative functions. The Emergency Call Centre, with the short code 999, has already been installed to respond to any emergency call related to Police, Fire, and/or Ambulance services. Bangladesh Police has a long way to go in terms of ICT adoption and innovation. Its office and service automation are in its early stages, with ICT accounting for approximately 20% of all jobs performed. There will be challenges ahead in terms of providing more ICT training, procuring modern equipment, and motivating police officers to adopt e-policing. Goal Transform police services to the second stage of e-policing, where ICT will be used for 50% of jobs and service delivery. Target Establish a strong and secure network connection, such as a VPN, among all Bangladesh Police units. Use IT in core policing activities such as intelligence gathering, inquiry, investigation, and verification.

There are numerous branches of the Bangladesh Police that carry out various types of work. According to rumors, a specialist police unit was anticipated to start operations in 2018 and would be outfitted with open-source intelligence (OSINT) tools to mine any statements or postings that could be defamatory, could impair religious sentiment, or could be an infraction under the ICT Act. A 505-man fully-fledged specialized unit named the Cyber Crime Investigation Bureau has already received approval from the home ministry, and the import of OSINT is in the works, according to officials. Because it can monitor the vast cyber world in a short period of time, OSINT is unquestionably useful software for assisting police in locating cyber offenders.

Currently, police manually search for contentious items online. A search for "Bangladesh" on OSINT, for example, will return all social media posts or comments about Bangladesh. By changing the words in the search string, you can narrow down the search results. The OSINT is a data mining tool used for gathering intelligence from publicly available sources such as research, newspapers, and social media. The home ministry stated in a recent order that the cyber bureau was established to effectively deal with the growing number of cyber and pornography-related crimes.

In the last five years, approximately 1,417 cases were filed under the ICT Act against 2,873 people, according to the police headquarters. There were 19 in 2012, 48 in 2013, 149 in 2014, 303 in 2015, 546 in 2016, and 352 as of June 30, 2017. Investigators frequently fail to present evidence to show a crime because they lack knowledge in cybercrime, which leads to the accused being exonerated in 66% of cases. In the long run, he continued, a specialized police unit examining ICT matters may lead to sentencing in 75 to 80% of cases. The only body that hears these matters is the Cyber Tribunal, and in accordance with the ICT Act, police must either file charges after an investigation or submit a final report to that tribunal. The unit will look into crimes such as hacking into Facebook and Twitter accounts, posting defamatory pictures or videos on websites, hacking into online bank accounts, using abusive words on the internet, comments that offend religious sentiments, and other offenses.

In this pandemic situation, I could reach only the Special Branch (SB) of Police. So, this interview gives us a partial scenario of Bangladesh Police. Anyway, this section of police started practicing IT from 2012. They also follow National Information Security Policy guideline. They are yet to formulate Information security policy. They share criminal information from other branch of Police. They report to branch chief and if necessary, they inform to the Inspector General of Police.

Directorate of Land records and Survey (DLRS) has only 5 personnel in the IT cell. This office started their IT activities since 2011. Office of the DGLR uses state of the art information security system which is synchronized with ISO 27001. Director (Admin) usually looks after the section and s/he has been informed the situation, if any incident takes place.

### **6.3.1.2 Information Security Incidents, associated threats, and its consequence-**

Bangladesh, like other countries, is vulnerable to cyber-attacks. According to the Bangladesh Institute of Bank Management, more than half of the country's commercial banks are vulnerable to cyber-attacks. Bangladesh was recently the target of a large-scale, coordinated cyber-attack that targeted at least 147 public and private businesses, including banks and non-bank financial institutions (NBFIs), highlighting their vulnerability. The state-run Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) reported in a recent study that its cyber risk research team discovered flaws in over 200 Microsoft Exchange Servers (MES) in use in Bangladesh, categorizing the hazard level as 'high.' Bangladesh Bank (BB), Bangladesh Telecommunication Regulatory Commission, Lanka Bangla Finance, Standard Bank, Trust Bank, Bank Asia, Dhaka Bank, Evercare Management Group, Evercare Hospital Dhaka, Bangla Trac Communications, and Agni Systems, among others, are among the organizations mentioned in the report. Hackers breached Bangladesh Bank's networks in February 2016, using the SWIFT messaging network to change a \$951 million payment from the central bank's account with the Federal Reserve Bank of New York.

In the wake of the reserve heist by the BB, the government established the BGD e-Gov CIRT under the Ministry of Posts, Telecommunications, and Information Technology. By developing incident management capabilities that will enhance the usability of these services, the BGD e-GOV CIRT's mission is to support the government in progressing and extending ICT projects in Bangladesh. The following services are provided to its constituents by BGD e-GOV CIRT in order to achieve its goal: a) Security analyses on explicit formal request, the constituency may receive these services from the BGD e-GOV CIRT, which routinely conducts vulnerability assessments and penetration tests on assets located in the National Data Center. establishing and maintaining security settings for tools, programs, systems, and services: The BGD e-GOV CIRT maintains a documented set of security tools that are largely used for log gathering and archiving for assets in the National Data Center, allowing events to be traced when they happen; Intrusion detection: The BGD e-GOV CIRT collects cyber security threat information (compromises, accessible vulnerabilities) from a variety of sources, filters it, and distributes it to the constituency. Consultation on security: The BGD e-GOV CIRT provides advice and

guidance to constituents on how to apply the best security measures for their commercial operations.

**Increasing awareness:** The BGD e-GOV CIRT is looking for ways to enhance security awareness by generating articles, posters, newsletters, websites, and other instructional tools that explain security best practices and provide advice on how to avoid common pitfalls. Meetings and seminars may be held to keep stakeholders informed about current security processes and potential risks to organizational systems. A sensor network is being built in the Bangladesh government IP network to detect intrusion, suspicious behavior, and establish methodology for analyzing the maturity level of Critical Information Infrastructure.

**Reactive Services - Handling Cyber Security Incidents:** The BGD e-GOV CIRT receives information about cyber security incidents, triages them, and coordinates responses. The incident handling unit provides the following services: Vulnerability Assessment, Penetration Testing, Incident Analysis, Security Threat Notification, and Incident Coordination are all steps in the vulnerability assessment process. The Digital Forensic Lab at BGD e-GOV CIRT can now recover and investigate data from digital devices like phones, computers, drones, and other IoT or computational devices. The Service Workflow is as follows: Detection of evidence, collection of evidence, evidence analysis/examination, documenting, and reporting.

To fight cyber occurrences and enhance the state's cyber security landscape, the agency collaborates with numerous government institutions, critical information infrastructures (CII), financial organizations, police agencies, academia, and civil society. The BGD e-GOV CIRT receives information about cyber security incidents, triages them, and coordinates responses. The following services are provided by the incident handling unit:

a) **Vulnerability Assessment:** Constantly performing vulnerability assessments to find and measure the severity of vulnerabilities on assets located at the National Data Center, as well as providing these activities to the constituency on a special official request,

b) **Penetration Test:** Conducts penetration tests to breach security defenses on assets and provides vulnerability remediation by signing rules of engagement with constituency,



c) Incident Analysis: Analyze incident evidence to determine the root cause of the attacker's attack and provide best practice guidance to prevent future attacks,

d) Security Threat Notification: Receives cyber security threat information from trusted sources such as zero-day vulnerabilities, malware information, ransomware infection details, and so on, filters, and distributes it to the constituency,

e) Incident Coordination: Receives incident notifications related to BGD e-GOV CIRT constituent networks from trusted CERT communities and forwards them to the concerned constituents for mitigation.

In order to undertake forensic analyses on digital data, another unit—the Forensic Lab—was created in 2018. It offers forensic support on incident-related evidence as a reactive service after an incident, helping the incident handling unit.

The Digital Forensic team is also capable of recovering and analyzing data from digital gadgets including smartphones, computers, drones, and other Internet of Things (IoT) or computational devices. Additionally, CIRT LAB seeks to advance the knowledge and abilities of government employees and students with an interest in cyber security and digital forensics. Awareness is the state of being able to directly know, observe, experience, or be aware of events. It is the condition of being aware of something in a more general way.

The primary goal of awareness is to inform the end user about the current cyber threat and how to mitigate it. It is extremely difficult to reach out to every person and inform them about every incident of cyber security or cyber threat on a continuous basis. The BGD e-GOV CIRT is also working to raise awareness among its constituents. It issues posters, leaflets, newsletters, and web sites that explain best practices in security and offer advice on precautions to take. For a better understanding of its stakeholders, it publishes awareness articles in both English and the local language. It frequently published reports on the evaluation of stakeholder applications, including vulnerabilities and weaknesses. In addition, quarterly, semi-annual, and annual reports are published. For its constituents, BGD e-GOV CIRT organizes workshops, seminars, and conferences. It organizes different levels of training sessions for different stakeholders in order to prepare them. The training keeps stakeholders up to date on current security issues and potential threats to information security.

Cyber Range is another service of BGD e-GOVT CIRT. A cyber range is a simulation platform used to educate cyber security students, train and evaluate cyber security practitioners, and test processes and technologies in a real-world environment that simulates attacks, scenarios, and networks. Cyber Ranges give trainees hands-on experience with security products, allowing them to practice detecting, investigating, and responding to cyber-attacks. Cyber ranges are interactive, simulated representations of a company's local network, system, tools, and applications that are linked to a simulated Internet level environment. They provide a secure environment for product development and security posture testing, as well as a safe, legal environment for gaining hands-on cyber skills. A cyber range may include physical hardware and software, or it may be a hybrid of physical and virtual components. The Risk Unit assesses cyber security risks for Critical Information Infrastructure (CIIs) by identifying, analyzing, and evaluating risk. It assists CIIs in ensuring that the cyber security controls they select are appropriate for the risks they face. The Cyber Sensor Unit is implementing a sensor network to detect intrusion, suspicious activity, and to develop a methodology for assessing the maturity level of Critical Information Infrastructure in the Bangladesh government IP network. The main advantage of deploying a cyber sensor is the ability to "identify cyber security threats" within the organization (where the cyber sensor is placed), such as monitoring IP network activity, detecting unwanted traffic in the network, and detecting suspicious/malware related executable downloads into the network. In addition, the cyber sensor provides a fast indexing and graphical review platform for indexing all events for deeper analysis. BGD e-GOV CIRT's Cyber Threat Intelligence Unit works with information about threats and threat actors to help mitigate harmful events in Bangladesh's cyberspace. The cyber threat intelligence unit collects and analyzes data from open-source intelligence, social media intelligence, and deep and dark web intelligence. They are currently collaborating with several renowned threat intelligence services and providing regular reports to the CII, financial institutions, and government.

The IT Audit unit's scope is to provide audit services in accordance with the Professional Practice of Auditing. IT audits typically cover Data Center (DC), Disaster Recovery (DR) Site, IT Infrastructure risk-based assurance audits, and consultancy services to perform audit services and assess requirements in accordance with International Standards such as ISO 27001/20000. The scope is not a

certification audit for any international standard, but rather to enable/assist the organization in achieving or practicing IT service processes standards such as ISO 27001/20000 and other best practices. The CIRT audit and/or consultancy service will constantly improve proficiency, risk management, governance, IT effectiveness, internal control, and the quality of IT services. To add to and protect the value of an organization by providing risk-based and objective assurance, advice, and insight. The Cyber Security Policy Development Unit creates cyber security policies, frameworks, standards, controls, and guidelines. Distributing them to appropriate authorities, as well as providing regular training and monitoring.

Its most recent assessment blamed the current incident on Hafnium, a hacker organization, as well as other threat actors, while naming Windows operating systems, notably MES, as the attack source. Tarique M Barkatullah, director (CA and Security) of the Bangladesh Computer Council, told The Financial Express that it was unknown what types of information were stolen from the organizations (that came under the latest attacks). He described it as a major problem, noting that Hafnium and other threat actors broke into organizations' emails in order to steal their data. The attacks were carried out not only in Bangladesh, but also around the world, with hackers exploiting MES flaws. Mr. Barkatullah, who is also the Digital Security Agency's director of operations, stated that the businesses involved should take preventive measures to avoid further assaults. He asked all other organizations, including banks and non-bank financial institutions, to tighten their security procedures in this regard.

Respondents from Bangladesh Bank confirm that they were not so affected by any major occurrence related to highly breach of information since a couple of years back. However, they experienced usual minor threats which nowadays have become common phenomenon to the Bangladesh perspective. Bangladesh Bank has its own CIRT, and report explains that IT personnel in various financial sectors faced problem with Spam, Ransomware, Phishing, DDoS, Data breach, identity theft, web-based attack and so many things like that. Spam as well as Ransomware and Phishing is the most frequently experienced and encountered phenomena and they significantly impact critical information by causing huge loss to the financial bodies. BB interviewee then added that attempts to hack by Black hat hackers, unaware or careless employees and outdated security controls are often the most vulnerable part of security systems. The system is moderately secured, not sufficient.

Election Commission of Bangladesh confirmed that they have not been suffered by any information incidents yet. However, they experienced Denial of Services (DoS), Web Based Attacks, Botnets and Crypto jacking type threats. Those attacks are intended to modify the integrity of critical information. Election commission uses cloud servers as well as maintain well backup of data. The respondents opined that Malware, Phishing and e-mail viruses are the most perceived risk for their organization but at the same time they claim the system is sufficiently secured.

In this regard Special Branch of Bangladesh Police reiterated that till now their organizations had no track record of hacking. Although, from the very beginning they maintain/share criminal information, they, however, recognize presence of malware in their systems. Sometimes Information leakage by the employees makes them embarrassed. Other than this, the incident of cyber espionage and insider threat may take place. The SB office of Bangladesh Police apprehends that these incidents affect them with damage of reputation as well as loss of crucial information about notorious criminals. Despite having such anxiety, this wing of Police believes that their system to some extent secure.

While providing data on IS, contender from DLRS office echoed that directorate of land records and survey deals with important information like title of land, positioning in the *mouza* map and genuine area of land. Most of the cases, land litigation arises from false information. So, they have to take extra care about CIA of land information. Even then, there were some incidents of Physical manipulation and Data Breach. Those events ruined their prestige and at the same time cause sufferings to the general people. Having learnt from the lessons, DGLR office now claims that they maintain well-equipped security systems.

#### **6.3.1.3 Preventive technologies-**

Bangladesh is preparing to implement a cybersecurity plan with the goal of creating circumstances for the safe operation of cyberspace by increasing vulnerability to the increasing threat of cyber-attacks. The Bangladesh Cybersecurity Strategy for 2021-2025 has already been written by the Digital Security Agency, which is part of the Information and Communication Technology (ICT) Division. The ICT Division will shortly present the strategy to the cabinet for approval, after making any required

revisions based on input from other stakeholders, officials involved told The Business Standard (TBS). The proposed cybersecurity strategy, the first of its type in Bangladesh, promises that all ministries will be outfitted with specialized software and qualified personnel to protect themselves from cyber-attacks. The government has launched the program at a time when all countries, including the United States, are concerned about cyberspace safety. The National Cybersecurity Strategy of neighboring India is likewise awaiting approval by the cabinet. According to ICT Division authorities, the proposed strategy focuses on ten elements to address future cyber issues and strengthen the country's cyber capacity. The review article's major goals include getting better national cybersecurity governance and ecosystem, improving organizational management and business operations, strengthening cybersecurity incident management and active cyber defense, strengthening national cybersecurity capacity, nourishing cybersecurity knowledge through education, and promoting a competitive local industry and ecology. According to the paper, under the supervision of the education ministry, 250 graduates and 125 postgraduates, including 25 Doctors of Philosophy (PhDs) in cybersecurity, will graduate from public universities each year. According to authorities involved, the ICT division will write letters to all ministries seeking views on the draft strategy by this week, and the department will make required changes or additions to the document based on stakeholder suggestions before sending it to the cabinet. Md Mostofa Akbar, Professor of computer science and engineering at Bangladesh University of Engineering and Technology (BUET), agreed that Bangladesh is an emerging leader in cyber security since it has improved in attack prevention. However, the country may face large-scale attacks and dangers in the future, he told TBS, adding that the national cybersecurity policy will aid in protecting Bangladesh from hackers and other risks.

Interviewees from BB again stated that they use latest operating system (OS) and updated 1st party anti-virus and patch to prevent internet-based incidents. Furthermore, as soon as they noticed that their systems get infected, they disconnect the device from the net system and shut it down. While doing so, they prepare documentation of the scenario of incidents in written form in order to make investigation later. In this situation, IT personnel are supposed to perform activities according to the 'Guideline on ICT security for Banks and non-Bank Financial

Institutions, May-2015'. For anticipation, they usually get alarm/notice from n-CIRT and various online scientific journals. Employees of IT section have academic background of ICT. Moreover, they are provided with compulsory training according to the BB's aforesaid guideline.

EC of Bangladesh claims that with a view to smooth practice of IT governance in their organization they maintain an inclusive effective configuration of ITIL, CoBIT and ISO/IEC 27002. The organization heavily depends on international best practices such as ISO series of guidelines and principals. COBIT, an acronym for Control Objectives for Information and Related Technologies, was first introduced in 1996 as a set of practices and guidelines to assist management in getting the most out of IT resources. COBIT, also known as a framework or a methodology, bridges the gap between IT goals and business goals by providing resources to build, oversee, and improve its implementation while lowering costs, maintaining privacy standards, and providing structure and oversight to the organization's IT functions. ITIL is an acronym that stands for Information Technology Infrastructure Library. It is a framework designed to manage an organization's IT services across the entire lifecycle by utilizing a set of best practices, planning, and selection. ITIL focuses on IT service management or dealing with problems from the standpoint of the IT department. ITIL assists businesses in organizing the daily processes and routines of their IT teams. To prevent upcoming threats, they paid special concentration on recent presentation and discussion of conferences on security awareness. Furthermore, sometimes vendors warn them well ahead of an organized attack. They also have provision of regular employee training on IT audit and management. ISO/IEC 27002 provides guidelines for organizational information security standards and information security management practices such as control selection, implementation, and management while taking the organization's information security risk environment into account (s).

SB of Bangladesh Police mention that they use open-source software which prone to less vulnerable. Though they have yet to formulate any organizational security policy, they usually follow international best practices. IT personnel of EC have a keen eye upon the latest security trends through several online sources. They have expert on IDS who examine the system on regular interval. Each year they spent a handsome amount of budget to make their people IT aware.

IT professionals of DLRS remarks that they always use updated version of licensed software which have latest release of patches. They always abide by the rules of government published ISPG for data management. This office depends on governments warning systems for predicting of new threats and vulnerabilities. In addition, they always monitor system performance, responsiveness and integrity of data & transaction volume. In order to detect attack, their experts check database in binary data layer, abnormal resource usage (real time) and presence of malicious code in their system. All staff including IT people are getting security training according to the government policy.

#### **6.3.1.4 Safeguarding and Reactive measures to the incidents-**

BB interviewees confirm that they have been practicing DPI for several years. A part of network packet filtering is DPI. Deep packet inspection checks a packet's data and header as it travels through an inspection point to weed out any protocol violations, spam, viruses, intrusions, and other predetermined criteria that could otherwise prevent the packet from passing through the inspection point. In order to decide whether a certain packet needs to be forwarded to a different location, deep packet inspection is also performed. Deep packet inspection may find, detect, classify, stop, or reroute packets that contain specific code or data payloads, which standard packet filtering cannot do. Deep packet inspection, as opposed to simple packet filtering, goes beyond simply inspecting packet headers. Using rules that the user, administrator, or internet service provider has preprogrammed, DPI checks the contents of data packets (ISP). It then decides how to respond to the risks it has identified. Based on the contents of the packet and its header, DPI can not only identify the presence of threats but also pinpoint their origin. The application or service that first exposed the threat can then be identified by DPI. DPI can also be set up to employ filters, which enables it to recognize and reroute network traffic coming from a particular website or IP address. Traditional packet filtering can only read the data that is included in the header information for each data packet. This is a simple, less complicated solution due to early technical limitations. Because firewalls could not process huge volumes of data fast, they were only concerned with the header information because anything more would need additional labor and time, which was an unacceptable cost to network performance. However, as new technologies emerged, it became possible to carry out more thorough packet scans in real time.

Now BB authority has established much control on the component of each data packet passing through e-mail or their intra/internet system. In addition to that, they exercise pen test of the system in every alternative month with a view to explore vulnerabilities. Another control point is to safeguard third parties (e.g., partners and suppliers) acquiescence with suitable security customary. BB confirms a sufficient and proper degree of security over third parties through ISO 27001:2005 certification and accomplishes random spot check on vendor's sites. ISO 27001:2005 is applicable to all kinds of businesses (e.g., commercial enterprises, government agencies, not-for-profit organizations). Thinking the organization's total business risks, ISO 27001:2005 outlines the specifications for creating, putting into practice, running, monitoring, reviewing, maintaining, and upgrading a documented information security management system. It outlines the conditions for putting in place security measures that are specific to the needs of organizations or segments of them. The goal of ISO 27001:2005 is to guarantee the selection of appropriate and proportionate security procedures that safeguard information assets and inspire confidence in interested parties. BB as well as all other financial institutions now direly needs locally prepared software and security patches. At the end of the interview, BB personnel expressed their satisfaction with the positive attitude of the convinced management for increased allocation of budget in security solutions.

EC of Bangladesh also has intrusion prevention system which they perform with open-source software. They always monitor suspicious e-mail and packet data in their system. An intrusion prevention system (IPS) is a type of network security that detects and prevents known threats. Intrusion prevention systems continuously monitor your network for potential malicious incidents and collect data on them. The IPS notifies system administrators of these events and takes preventative measures, such as closing access points and configuring firewalls, to prevent future attacks. IPS solutions can also be used to detect flaws in corporate security policies, discouraging employees and network visitors from breaking the rules outlined in these policies. With so many access points on a typical business network, it is critical to have a method to monitor for signs of potential violations, incidents, and imminent threats. Today's network threats are becoming increasingly sophisticated, with the ability to penetrate even the most robust security solutions. Sometimes they use self-develop tools to identify nature of incidents in the system. They usually control third party



access to the database to maintain data integrity. EC has a plan to establish a full-fledged encrypted intra network up to upazila level and run the system with local expert. EC respondents are also happy with the allocation they receive in order to maintain IT security for their office.

SB of Bangladesh Police doesn't have DPI system instead they use strong firewall and packet filter for their database. A network interface's ability to pass or reject packets based on their source and destination addresses, ports, or protocols is known as packet filtering. Together with packet modification and network address translation, the technique is employed (NAT). A firewall program commonly uses packet filtering to guard against unauthorized access to a local network. No penetration test has ever been performed in SB office. To ensure appropriated level of security over IT dealers they usually impose corporate security policy and mitigate the risks in the contractual agreement. For real time data sharing, SB needs a good network among all police stations in Bangladesh. They have insufficiency in both human resource (IT expert) & allocation of budget and office management is fully aware of the issue.

Respondents from the DLRS claim that they execute DPI in every now and then. This office also facilitated with regular penetration testing to their whole connected system. Interviewees also specify that regulating of third party is confirmed through access policy, review, spot check, audit and to some extent asked them to show certification. They have also emphasized for locally made software to impose more securitization. At the end of the interview, they replied that they have enough budget allocation for IT security.

## **6.4 Personal Observation**

This researcher is a civil servant and has been serving for Bangladesh government for last more than 24 (twenty-four) years. From the service experience in both field administration and Bangladesh Secretariat, there were opportunities to observe the practices of Information Technology in Government organizations. In fact, Bangladesh public offices adopted Computer in late 90s of the previous century. Although initially it was only used for typing the documents instead of typewriter, however, as time passes away, now Bangladesh government has installed its own

state-of-the-art tier IV data center in order to preserve or archive official data/information.

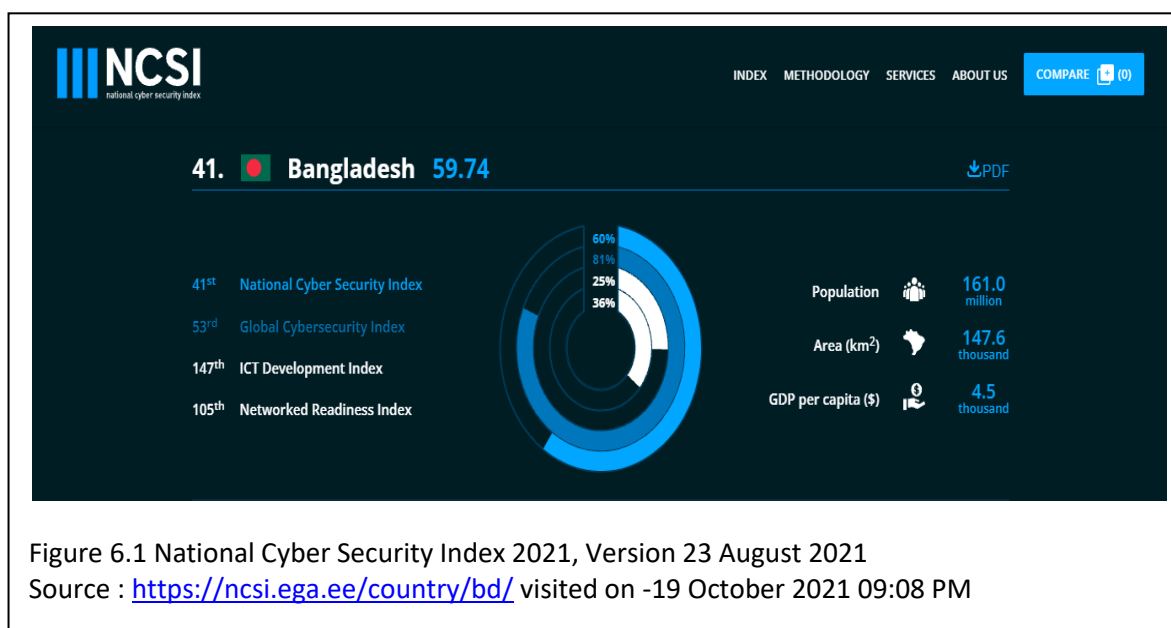
Right now, in Bangladesh Secretariat, from the Ministers to downward up to section administrative officers use computer to perform their day-to-day routine work. High officials like Joint Secretaries and above ranked officer are allowed to use laptop computer but below ranking officers use desktop PC on their table. Most of the computers contain non-licensed operating system (OS) and don't receive patch program from the vendors when needed which is more likely to be hacked at any time. Government staffs are well familiar with document typing and to some extent conversant with little third-parties software. Government employees are accustomed with smart phones and usually carry other portable devices and USB storages in their office bags. In most cases, employees show their apathetic nature while using strong password or two factor authentication to protect soft copies of important documents.

Large Ministries suffer from physical space crisis and sometimes more than one section has to be accommodated in a single room. Office staffs found far less serious about the confidentiality of information. Visitors, guests or interested parties have easy access to the sections and sometimes office staffs engage in gossiping with outsiders while flashing valuable documents on their computer screen. It is also evident that visitors are found looking into important decision-making files in the office room even in absence of any responsible officer present there. Though CCTV cameras are there on the lobby however inside the sections there are no surveillance systems. Public information security scenarios get even much worse in pandemic period.

In the Covid-19 intensified period, Organizations had to face several challenges. When the pandemic broke out, people got infected suddenly. The challenge exaggerated as the key IT personnel fall into illness or quarantined or disappeared in the office due to fear of Covid-19 infection. On this perspective, Bangladesh Secretariat was shut off for several months at a stretch caused a huge gap for routine maintenance of Computers and related accessories. Employees were asked to perform essential official job staying their home in lockdown situation. At that time, they were compelled to use their less protected home devices and unencrypted online network to share their work with other colleagues. This entire situation made government critical information more vulnerable and prone to leak to the hackers.

## 6.5 Key Informant Interview

I selected Mr. Tarique M Barkatullah, PD of BGD e-GOV CIRT under the ICT division of MoPTIT as the key informant of this study. He has been working on Cyber Security for Bangladesh government for several years. Mr. Barkatullah said that the country's capability in cyber security is increasing day by day and thus gaining recognition in the world.



### 6.5.1 Experienced on-going Risks, Threats and Vulnerabilities

Bangladesh has scored the top position among SAARC nations in the National Cyber Security Index (NCSI); reports UNB. NCSI evaluates cyber incidents, by being ready, you can avoid common cyberattacks, crimes and carry out essential crisis management procedures. In reality, Bangladesh rose 24 places in the NCSI of the Estonia-based e-Governance Academy Foundation in 2021, taking the top spot. Bangladesh presently ranks 41st out of 160 nations, earning a score of 59.74. (Annexure II). In the December 2020 index, Bangladesh was rated 65th.

Information threat is an emergent risk that is snowballing day by day. New threats are appearing to the horizon and old ones are sprouting in respect of time and technology.

With the convenience of hacking as a service and more free tools to produce scripts along with other threats spontaneously make attack easier even for the beginner. These growing threats are also influencing Bangladesh eventually as we are also habituating in the process of globalization.

Table 6.1 Top Information Threats in Bangladesh 2020

<b>Serial no.</b>	<b>Top Information Threats</b>	<b>Serial no.</b>	<b>Top Information Threats</b>
01.	Spam	02.	Ransomware
03.	Phishing	04.	Malware
05.	Information Leakage	06.	Insider Threat
07.	Identity Theft	08.	Web based attack
09.	Data Breach	10.	Denial of Services
11.	Web application attacks	12.	Botnets
13.	Crypto jacking	14.	Physical manipulation/theft/loss
15.	Cyber Espionage		

Source: Bangladesh Cyber Threat Landscape 2020 pp.5

It is essential to understand the new cyber challenges and anticipate the future attacks and permit prolific reaction to the upcoming cyber threats. Each year reputed international organization like ENISA as well as business service providers circulate lots of cyber risks, threats and vulnerabilities.

With a view to precede with the necessary cyber capabilities and effectively reduce threats and vulnerabilities, every nation has their own strategies. It is necessary to understand own cyber threat scenario based on local data structure. We must be more careful on eminent risks, their collaboration with threat mechanism and inter/intranet vulnerabilities

### **6.5.2 The results of Existing Protection Mechanisms**

KI argues that the risk in cybersecurity is always unpredictable. It has got exaggerated as the Covid-19 pandemic has altered the way institutions measure risks and react to the threats. Threat players are fully aware that people have been working remotely from their offices and they are more likely to be vulnerable. He then added that security events intricate unpatched software vulnerabilities, and enterprise-level organizations face security occurrences caused from misconfigured services or systems.

As enterprise employees modified their equipment and security systems to fine-tune to these threats, hackers in turn are anticipated to transform their strategies to find new flaws with remotely used devices. Consequently, institutions are revising their vulnerability assessment and response strategies. He claimed that most organizations may fail to meet addressing information threat and vulnerability. More precisely, a good number of CEOs believe their risk response performances are under-financed.

In this connection, KI expressed his firm belief that Information Security budget might be unchanged for addressing post-pandemic vulnerabilities and threats.

### **6.5.3 Information Security Consciousness inside the Institutions**

Organization's administration is accountable for confirming that an applicable information security responsiveness and training program is delivered to employees. Without organizational backing, IT security staffs might not have adequate resources to expedite attentiveness and teaching for other workforces. Consciousness and understanding may vitiate over the time without continuing apprise of training and updates. Providing enduring information security awareness and training will assist in keeping employees aware of issues and their responsibilities

### **6.5.4 Auditing and Testing of Information Security Policies**

Uninterrupted IT auditing is a continuous monitoring method that permits IT auditors to inspect controls on a regular basis and to collect some careful audit indication through the system. Hypothetically, in some offices it may be possible to meaningfully reduce the audit reporting time frame to extract nearly sudden or actually constant assertion. In precise, nonstop assertion is more suitable for practice in high-risk, high-volume, less paper situations. As a procedure, constant auditing is

considered to allow IT auditors to make document on the subject within a much shorter time frame than under other audit models. As a process, continuous auditing can be adopted to allow timely reporting by IT auditors through nonstop testing.

### 6.5.5 Organization’s thinking on Better Security Policy

The key informant emphasized for an institution’s information security policy. It should not only carry a course of action, e.g. its determination, objectives, implement ability, status and performances; more significantly organizations should also make it clear about employees’ ultimate responsibility for executing the security outline.

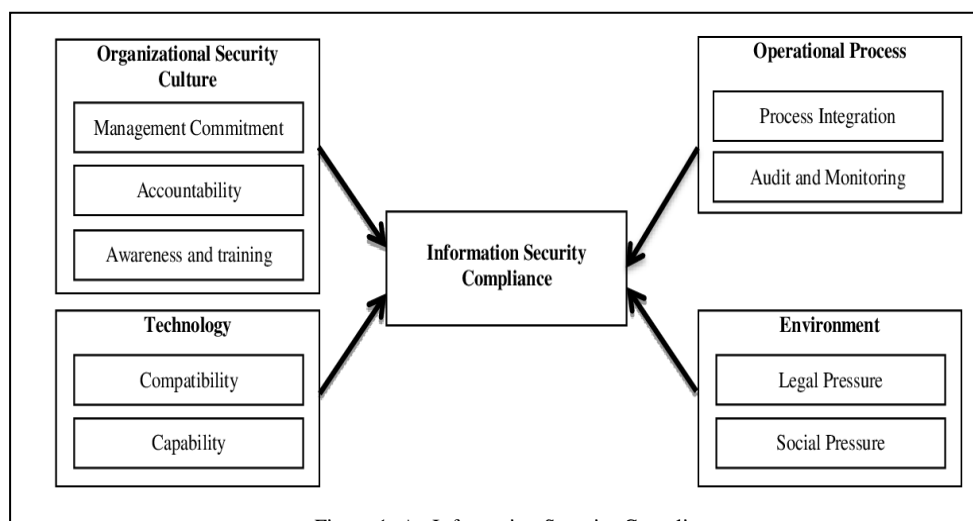


Figure 6.2 Information Security Compliance structure of an organization

All staffs within the office should be conveyed suitable drill on information security policy and the office’s security expectations, affiliated to their efficient roles. Again, the organization’s information procedure policy should be transferred into a flawless way, carefully read, clearly understood and recognized by all employees within the business environment. It is also authoritative for administrations to disseminate the rules, policies and processes through staff corroboration, as it delivers invaluable input into policy implementation and learning processes.

### 6.5.6 Business Continuity plan for disaster events

Key Informant then underscores the need for a good business continuity plan. According to the Information Policy Security Guideline 2014, every government organization should have such a preparedness plan to counteract against any kind of possibly disrupting incidents like pandemic, power shutdowns, fire, and hostile

weather etc. CISO will maintain communication with staffs, customers and service seekers and should send news updates and links to civic resources to keep personnel informed of the latest status of the pandemic and best practices for continuing a sound and vigorous office atmosphere.

## 6.6 Major Findings

- Public organizations in Bangladesh adopted Information technology extensively for Information management in 2010 but IT securitization processes practiced much earlier.
- For Information Security compliance, Government institutions are supposed to follow Information Security Policy Guidelines 2014 and for best practices renowned enterprises track ISO 27K series standards/frameworks.
- There are adequate Acts, Policies, Standards, Guidelines, Strategic implementation plans are in place to secure Bangladesh government's CII.
- Many institutions are now formed CIRT under BGD e-Gov CIRT of BCC. Mother CIRT provides information and alarm notices to different organizations about new (possible) attack.
- Although they use extra lair security features in devices however a big number of computers used in Bangladesh Secretariat (the hub of country's administration) don't have licensed OS as well as regular patch programs.
- Employees are less motivated to secure critical information such as e-mail, e-*nothi* (file), e-GP (Government Procurement), and PMIS accounts.
- In the Covid-19 pandemic situation, Bangladesh experienced mostly Spam along with Phishing and Ransomware attack in its network system although there is no track record of huge damage/loss/threats of Information assets.
- Regular IT audit and penetration testing for local servers rarely take place in public offices.
- The (draft) Data Privacy Act has yet to be finalized.

## **CHAPTER VII: DISCUSSION AND WAYS FORWARD**

### **7.1 Overview**

From the previous chapter we have got so many findings through a rigorous analysis of interview data and secondary evidence. Now, based on the findings there will be a critical discussion in order to portrait a crystal-clear security scenario and at the same time find the means to get rid of. It is an undoubted fact that Bangladesh has made tremendous progress in global cyber security position. But there are lot of things to secure sensitive as well as personal information.

### **7.2 Emerging Critical Threats**

#### **7.2.1 General symptoms related to cyber/malware attack in a device**

It is due to hacker's skill; users sometimes do not notice about the cyber incidence. However, there are some indications by which it could be recognized. Those are-

- ❖ Popup windows get open automatically.
- ❖ There is a new home page on the web browser.
- ❖ Automatically added new tool bar to the browser.
- ❖ System crash may take place unexpectedly.
- ❖ Unknown programs enabled in the device.
- ❖ Spontaneously disable anti-malware functions.
- ❖ Gradually computer performance gets slow.
- ❖ Unanticipated request for new password validation.
- ❖ Folder/files and memory storages get encrypted and lost access control.
- ❖ Deletion of files and/or change in content.
- ❖ Redirected of internet search.
- ❖ Automatically scanning with an unknown anti-virus system

#### **7.2.2 What to do instantly if the systems get infected**

- Disconnect the device from all sorts of internet network.
- Detach the computer/laptop from all types of remote access session.
- Shut down the system.
- Record the suspicious activities.



- Communicate with the service provider or the head of the security branch of the organization.

### **7.3 Impact of Covid-19 on Organizations Information Security Budget**

COVID-19 has made people more dependent on the internet than they have ever been. During times of lockdown, and while social separation is advocated, internet architecture has emerged as the primary focus for communication, trade, business, and learning. Covid-19 has made serious impact on organizational Information security. When the pandemic upraised, Government was compelled to impose lockdown with a view to prevent its spread in the society. All sort of financial activities including government offices came to a halt for several months. While companies swiftly adapted to this transformation in order to keep their processes operating, and people gained adapted to remote working and e-commerce, computer hackers have also taken benefit of the shift in online practices. However, utmost important offices of the state were to remain open for the sake of public interest. Those employees had been asked to perform office work staying in their home. Some of the work was highly confidential and urgent in nature. But the unencrypted documents were not shared in a VPN or any other secured network. Therefore, the sensitive documents fall into vulnerabilities and prone to be compromised as the home networks of the office staffs were not flawless. In addition to that home computers are usually open to family members and in most cases, they are not aware of the value of that Information. According to Europol's 'Internet Organized Crime Threat Assessment,' cybercrime has been on the rise all year. This trend, however, is not surprising given that hostile actors have always been enterprising and clever, altering their strategy to increase success rates. The COVID-19 situation has been no exception.

According to Interpol, the crisis has resulted in a dramatic change in target from individuals and small enterprises to huge organizations, governments, and key infrastructure. Business sustainability has long been a top issue for many businesses and their IT departments. However, the COVID-19 situation has put a strain on budgets, exposed flaws in cyber security defenses, and highlighted the IT skills shortage. As a result of the crisis, departmental budgets are still being squeezed, and resources for less critical operations are being cut—a circumstance that we predict will shape spending in fiscal year 2021, which many departments are already planning

for. Total expenditures should slow off from the sector's recent strong rise in businesses that were heavily struck by the COVID-19 issue, according to new McKinsey research, while remaining stable in areas that were not as hard afflicted.

The problems that cybersecurity businesses are dealing with have spread to technology providers. Those businesses have made their own pivots to stay up with changing client needs and implement new business practices. Technology companies must rethink their strategy and offerings to meet a new safety landscape in the post-COVID-19 future if they are to succeed. They must also keep an eye on their customers' needs and adjust training, service, and sales accordingly. Following the pandemic, CISOs implemented actions right away to guarantee business continuity and safeguard against new cyberthreats. In order to guarantee continuity, they have been patching distant systems via virtual private networks (VPNs) that have suffered under increased load. They have been monitoring increasing danger levels since the crisis started, including a nearly sevenfold rise in spear-phishing attacks. Remote workers are also being targeted by assaults based on COVID-19-crisis themes, which take advantage of delayed email and web filter upgrades and use social engineering to play on employee anxieties.

Moreover, a fresh survey report conducted by IDG 2020 published in its 'Security Priority Study' in last December reveals that directing compliances and best practices are perhaps the two important spend factor for organizations in post-pandemic period. The report also mentioned that whether the budgets figure increase or decrease, CEOs will be more focused on personnel training and security consultants. The automation software, operating systems and other services (e.g., digital procurement, online financial transaction etc.) will make up the bulk security spending in government organizations.

The report concluded with the sayings that it might take another year for institutions to reappearance to pre-pandemic security strategies, but maybe with changes for the better.

## 7.4 Best Practices to handle Information Incidents

The confidentiality lies at the heart of data protection law. Privacy and data protection are considered essential rights. The security of a person's personal data is part of his or her "private life." Personal data is defined as information that distinguishes or is related to a specific person. Data is regarded the new money in the age of the fourth industrial revolution. Every day, the quantity of data collected and processed increases at an exponential rate, and data-driven revolutionary technologies such as Artificial Intelligence, the Internet of Things, and Big Data continue to test the legal framework in every country. The goal of incident response is to identify genuine security incidents, bring the situation under control, limit the damage caused by an attacker, and reduce recovery time and costs. Incident response management frequently includes formal paperwork outlining incident response protocols. The entire incident response process, including planning, detection, analysis, containment, and cleanup following the incident, should be covered by these processes.

Organizations can limit damage, prevent further losses, and comply with applicable compliance regulations by following these procedures. Create an incident response plan for your business in case one is experienced, as data breaches are becoming more frequent. Organizations employ incident response plans to outline the actions they will take in the case of a data breach or any kind of danger to data security. The procedures may differ depending on the nature and seriousness of the danger, but they often involve initial containment, threat elimination, recovery, incident notification, and post-event review.

With the adoption of the Digital Security Act of 2018, Bangladesh has joined the framework for the protection of data or information. Personal data is defined as "identification information" in Section 26 of the Digital Security Act of 2018. For the purposes of collecting, marketing, storing/preserving, supplying, or exploiting an individual's identifying information, Section 26 requires that the individual's explicit agreement or authorization be obtained. To get there, providers should concentrate on the following critical areas:

#### **7.4.1 Common users**

In a pandemic situation like covid-19, government employees are supposed to perform their daily routine jobs staying at home. Home users always may not have the security privileges as they enjoy it sitting in their organizations. Official devices and information infrastructures usually are much more sophisticated than those of home ones. In these circumstances, general and common users may track the following rules:

- **Surprising or unsolicited emails-**

Employees have to be aware about incoming unexpected and voluntary e-mails even it comes from in the name of a known person or organizations.

- **Uses strange email addresses-**

It should not take into connivence of mails which contain abnormal and unusual salutation, text and put extra responsive when having spelling and grammatical mistakes.

- **Emails stressing urgency-**

More attention will be paid to those messages or e-mails where users are requested to click on a web link or subscribe with personal information.

- **Contains attachments-**

Attachments have to be verified with the senders. If they are not expected and don't come with the original mail, then those may cause harm to the recipient.

- **Embedded attached links-**

Users should be more thoughtful about the implanted links with the incoming communication messages. However, the safe alternative is to navigate to the mentioned organization's official website instead of using link on the email.

- **Deliver sensitive information-**

People should more attentive while provide critical information such as personal credentials, credit card number, addresses etc. Generally, a service organization is not supposed to ask you to submit such type of information through e-mail or phone.

- **Fake information-**

Employees can keep trust only the verified origin of information. Office staff should be aware about misinformation and disinformation.

- **Browser and plugins-**

Web browsers are considered the first point of internet communication. So it should be updated with the latest one and associated plugins are also necessary to keep efficient.

- **Block Pop-ups-**

Generally, browser popups open new window for commercial ad and in most cases, those are irritating and may contain malicious programs. As a common user, we should not click on a popup as it appears on the screen.

- **Delete unnecessary cookies-**

Since cookies contain much important information about the users, it is necessary to delete unnecessary cookies

- **Avoid torrenting sites-**

Torrenting and file sharing sites should be kept in disable as those sites could share user's information without any prior notice to the staffs.

- **Download-**

Necessary software, apps, audio-video could be downloaded only from trusted origin, sites or stores. Third party software are always harmful and should not use in government organization.

- **Logout-**

We must logout from the safe site after having finished our jobs.

- Follow the government e-mail regulations 2018

#### **7.4.2 Home users-**

- ✓ If possible, always use organization provided laptop for official purpose.
- ✓ Make sure that operating system (OS) as well as all the protection software, anti-virus and anti-malware, security patches are latest and updated.
- ✓ With a view to perform official jobs, employees should always connect with end-to-end encrypted and protected remote access to the institution's domain.

- ✓ Employees should be familiar with complex and strong passwords.
- ✓ Staffs should not use other web browsers for personal affairs as s/he is connected with remote access session. It could infect VPN network anytime.
- ✓ Never disable firewall or anti-malware system while performing public services.
- ✓ In this situation, public Wi-Fi system should be avoided.
- ✓ Screen lock could be imposed, or remote access may be stopped while computers/laptops are remaining idle.
- ✓ Family members, neighbors or any other person should not be allowed to use the device for any purpose.
- ✓ Passwords and passphrases would not be disclosed with family members and at the same time passwords would not be saved in a shared device.
- ✓ Enable two factor authentications for official important accounts as it always ensures an extra layer of protection.
- ✓ Photocopier, Printer, Fax machines have their own memory chips. Extra attention should be paid while using those type of devices.
- ✓ Always scan USB/ portable memory/ removal drives before using them.
- ✓ Avoid using PC speed booster or RAM cleaner

#### **7.4.3 Using social media-**

On the one hand, as social media provide so many opportunities to disseminate information to the general people, however, without much attention sometimes user has to experience huge sufferings. Disinformation always takes place in social media purposely. In this case, if the government officer's account is hacked by interested group(s), miserable then knows no bound. So, it is highly needed to keep institutional as well as personal account protected. Government employees need to follow the followings-

- Follow the guidelines for using of social media 2019 in government organizations,

- Not to accept friend requests in social media coming from unknown persons.
- Appropriately set privacy settings and examine it repeatedly.
- Select the viewer of a particular post carefully.
- Organize/reorganize friend lists.
- Not to post any answer, explanation, information, report, audio-video clips, photograph without prior approval from the office head of the government institution.
- Use alpha-numeric strong password according to the security policy.
- In case of log-in into official website/account, there should be two factor authentication enabled.
- Not to use the same password(s) for more than three months period.
- Use different passwords for different social media.
- Make sure of approval of an employee(s) while tagging him/her in a particular post.
- Utmost carefulness is needed while making comment or liking on a sensitive post.
- Maintain secrecy for personal information.
- Government employee(s) must log out from his personal account in case of using another device(s).
- To be more careful when using third party/ mobile application.
- Use updated apps/browsers for using social media.
- Before acting on the basis of any posted information in social media, it is necessary to validate its precision.

#### 7.4.4 Using smart phones

In the era of IT, smart phones are the daily essentials. No one as well as government staffs can't do without cell phone. Likewise, computers/laptops, security features are also necessary for smart phones as nowadays it may servers the purpose of a PC. Cyber criminals are also found various ways to hacked it. So much responsiveness also needed here in order to maintain proper security. The following points could be acknowledged-

- Not to use phone number or date of birth as a password rather biometric authentication may be a good idea.
- In order to find out lost phone, it is better to use anti-theft feature of the device.
- Operating systems along with used apps should always be maintained up to date with state-of-the-art released software.
- Necessary apps should be downloaded and installed from verified apps store.
- While installing, everyone should take extra cautious about letting the apps/software to use contact list, camera, microphone, gallery and other sensible parts of the device.
- Not to perform any financial transaction, official file disposal or likewise activities which is secret in nature using public Wi-Fi or hotspots.
- Always enable device tracking systems.
- Not to keep on GPS location or blue tooth systems unnecessarily.
- Not to let another unknown person using smart phone.
- Not to click on a mysterious link or respond to a spam call.
- Critical information should always be kept in encrypted mode.
- Not to reply any unfamiliar messages from smart phone.
- Use anti-malware from a verified/trusted sources



#### **7.4.5 Dealing with Employee (Human) Risks**

Every institution should try to deal with risks originated from its employees by implementing security know-hows and service delivery process (Colwill, 2009). Technology is not supposed to halt someone from clicking a web-link and processes to be overlooked. So, without a full attention on office staff's security strategy may fall in disappointment.

Employee training is thus which affects the office staffs, adjusts their behavior and instills a security attitude in their daily routine activities. An employee-centric awareness program complements the human components to complete the three-legged stool which support institutional security strategy (Dong et al., 2021).

#### **7.4.6 Protecting Employees from Covid-19**

In the on-going pandemic condition, employees of public organizations were asked to work remotely as the lockdown prevailed. In order to ensure information security, organizations should confirm VPN access to BMS for monitoring of remote data center. Government organizations have their SOP and EOP to facilitate remotely copilot of critical information. VPN provides optimum protection for e-mail, VoIP and audio-visual meetings for an urgent consultation. Chief Executive of the organization, in this case, should anticipate the challenges of smooth operation of his office with a smaller number of staffs. At the same time, employees would be aware of serving people strictly following pandemic protocol in every step. Travelling restrictions had been imposed on public servants with a view to prevent the extensive spread of this contagious disease. To keep the government office operational, authorities built some team and introduce shifting duties with their physical presence in the office once in a week. Inside the government offices visitors had to abide by 'No Mask No Service' and appropriate social distancing policy.

### **7.5 Develop Information Security Culture in Public Organizations**

The information sector is changing. At first, the emphasis was on technical solutions. The introduction of certifications such as ISO 27001 and Cyber Essentials then encouraged the development of policies, standards, and processes to improve cyber resilience. 'Human cyber' offerings have begun to proliferate in the last five years or so. Initially, these were created to meet the regulatory requirement for 'awareness

training.' However, this is changing as organizations that have invested in information technology and implemented good policies and processes are still seeing vulnerabilities stem from the operators of their IT, their workforce. There are more people online than ever before because a large portion of the workforce during the pandemic worked remotely. According to Interpol, the elevated connectivity has made it easier for cyber security threats to spread because of the sense of confinement, anxiety, and terror brought on by COVID-19. The Interpol Cybercrime Threat Response team has observed a sharp rise in the number of attempted ransomware attacks against important vital response infrastructure and organizations. Organizations should think about a broader strategy to make sure their workforce adopts the right behaviors in a future where many individuals may continue to work remotely on a regular basis. Leaders must focus on changing behavior through an information security culture rather than just raising awareness.

The term "information security culture" refers to an organization's workforce's attitudes, knowledge, assumptions, norms, and values regarding information security. These are influenced by the organization's goals, structure, policies, processes, and leadership. A good information security culture is one where both organizational factors of culture (policy, process, leadership, social norms, etc.) and the personal factors of culture (attitudes, knowledge, assumptions, etc.) align with the organization's approach to information security, manifesting in information security conscious behaviors. Recognizing that people, not technology, make an organization secure is critical to developing an effective information security culture. People are both the most effective countermeasure to cyber-attacks and the weakest link in information security chains. As a result, it is essential to foster an atmosphere where workers have the skills and instincts necessary to act as the first line of defense. An information mindset and an information culture help to foster employee pride, deliver growth through digital trust, and enhance an organization's reputation with customers. They promote an atmosphere where good information hygiene becomes the norm, making it easier for the entire organization to operate more securely and freeing up time and resources for essential operations.

The importance of security training and culture is becoming more widely recognized. We've seen this most often with clients in transportation, oil and gas, and other industries with a strong emphasis on safety culture. They've learned from establishing

a safety culture and are applying what they've learned to their information security interventions. Developing an information-oriented mindset and an information-secure culture entails more than just preventing attacks and breaches. It is all about instilling confidence in your customers and earning their trust. It's all about being a socially responsible business. It's also about taking care of your employees. Being knowledgeable about information is a skill that your people can apply in their personal lives and use to help their families.

### **7.5.1 Role of Organization's Governance**

The preventive actions for Information Security may be considered a strategic objective in a public organization. So, authorities should incorporate information risk issues into the administrative and financial planning processes of the organization. The procedures need to deal with turbulent or volatile situations that might arise following an incident.

### **7.5.2 Launching Framework for Security Awareness-**

With a view to effectively change personnel mindset and shape an IT security culture in an organization, an inclusive program is needed based on organizations vision and mission. To achieve this five steps package may be helpful-

7.5.2.1 Analyze- A complete analysis of a situation will provide information need to build a successful security awareness plan. To analyze and assess a people centric approach to security awareness, we have to concentrate on some data gathering methods. These are- Organizational goals, Organizational compliance, Stakeholder analysis, Scope of security awareness program, Employees level of security knowledge, assess employee's motivation level, support resources, actual need and cost of social awareness

7.5.2.2 Plan- Planning allows estimating and addressing the deterrence, stay aligned with organizational vision, stick to timeline and budget and ultimately be more guaranteed of success. There are six areas to be considered in a planning process- Team, Strategic roadmap, KPIs and metrics, Security products, communication and Business case.

7.5.2.3 Deploy- Security awareness program could be deployed in three phases- test, launch and strengthen. After successfully completion of testing, then comes the stage of inauguration. These help employees know about what to do and how to maintain its momentum. Then strengthening the campaign with some effective communication tools, helped official staffs changing their mindset towards security awareness gradually.

7.5.2.4 Measure- Evaluate the performance of security consciousness activities provide valuable information which is essential to improvement the situation. In this step, we should quantify performance, stakeholder satisfaction and compliance of the organization.

7.5.2.5 Optimize- One of the most noteworthy benefits of calculating performance, employee satisfaction and compliance is that we will get the context to identify areas for upgrading and start developing an action plan to fix them.

Without a procedural security awareness framework, it is hard to make people change their uncertain behavior. A framework is crafted to take everything into attention, particularly how people learn, adopt and maintain new mindset, which eventually leads to a culture of security awareness and intensely lesser employee-connected security breaches.

### **7.5.3 Skillful Information Security Professionals**

All public agencies should appoint very resilient personnel to tackle information risk, threats and vulnerabilities as well as the whole information system. In addition to that, more importance should be given on exploration to check inclination of the trained personnel adoption of new technological changes. Head of the office may also announce ToT method to escalate more skilled staffs and master trainers who will further develop their colleagues in a culturally complex institution. In this connection, secondary and tertiary level education curriculums need to be reviewed in accordance with the changing scenario of cyber incident. A research and enhanced innovation may contribute to the positive mind set of organizational professionals, protocols and standards.

#### **7.5.4 Organizational Information Security Policy**

According to the Government Information Security policy guideline- 2014, public organizations are compelled to formulate their own Information Security Policy and a Regulatory Framework. Regulatory frameworks are necessary for ensuring in order to keep public and critical national information infrastructures are safe and secured. The organization boss should proactively incorporate prevention mechanism of next generation threats in its security frameworks and planning booklets.

#### **7.5.5 Employee training and awareness**

A big chunk of secondary evidence supports that human (employees) are a strategic security chain's weakest link. Only technology and innovative service providing processes are not enough to protect an institution. There must be staff component in a information security strategy on an organization. It is now a fair necessity that employee training is a major factor for effective cyber security of organization. An organization might have state-of-the-art technology which is operated by a group of experienced technical team but without having user awareness and regular training activity, information security program may fall in havoc. Even an inattentive action of an unaware user can cause of compromise the system and CII of the entire organization.

On the other hand, effective employee training and awareness programs can have the following results:

- i. Employees develop their habit to comply with organizational IS policy.
- ii. Users approaches should be in line with the organizations overall cyber-security policies and procedures.
- iii. Staffs should maintain some thumb rules in their behavior, such as:
  - Not to open email attachments come from unknown source with executable files.
  - Always maintain back up their important files out of the common systems.
  - Not to connect personal electronic attires such as- USB drive, smartphones, and other devices to office information systems.

- Not to send any highly sensitive classified official document outside the organization.

The goals of an information security culture must be strategic, organizationally aligned, and risk aligned. With the above mentioned, Government organizations must understand the current information security culture within their organizations. Government organizations must investigate their lived culture, purpose, and values, as well as how they influence people's engagement with cyber risk. It is critical to understand the reality of where government organizations are starts with understanding mindsets and behavior. This allows government organizations to identify critical gaps and create a reform strategy. Leadership support is essential to the success of these initiatives. It is critical to emphasize the role of leaders in leading by example. People will follow where they buy into, actively embody, and advocate security consciousness. Awareness campaigns, on the other hand, will be undermined if the tone at the top is not aligned. It is critical that, as changes to government organizations' cyber culture are implemented, government organizations listen and adjust. Government organizations must continue to listen to their employees and understand how changes affect how they engage with cyber security. It will be easier for government organizations to make the necessary modifications to continue progressing toward their goals if they have an objective and honest assessment of how their efforts have fared. It also provides an opportunity for government organizations to celebrate successes and recognize positive shifts.

All these three strategies in association with the institutional security policy will contribute to a strong collective framework that ultimately secure sensitive information in Bangladesh government agencies. However, Information Security issues remain an exclusive concern that requires strong collaboration from all stakeholders inside the country and worldwide. Few organizations place a premium on security culture, which can lead to illogical decisions, compromised systems, and data breaches. Creating an information security culture is an ongoing process that requires participation from all levels of an organization. By implementing proper cybersecurity practices in the government organization, not only will a security culture develop over time, but the institution will also be kept safe against cyberattacks.

## CHAPTER VIII: RECOMMENDATIONS AND CONCLUSION

### 8.1 Overview

Technology has modified the way modern offices perform their duties and deliver services. To protect organizational assets, all employees inside the institution may be given the proper training on IS policy and the government's security outlooks, affiliated to their practical character of duties. It is necessary to maintain a balance between powerful, integrated and complicated security measures that is synchronized with skillful office staff and resources for the government organizations as such organizations has access to the national database. Therefore, modification/ theft of any such data leads to devastating effect on the overall society.

### 8.2 Recommendations

In order to mitigate third party risk, financial security in the state transaction process, safeguarding against ransomware attacks, maintaining synchronization with digital transformational endeavors- followings are some points that should consider of every Chief Information Security officer (CISO) of the organizations.

#### ❖ **Emphasis on Security Fundamentals-**

CISO of every organization have to make sure that fundamental elements of Information security are being observed strictly. Basic Security of organizations encompasses accomplishment of Information asset management, updated patching, checking system vulnerability, configuration of operating system as well as providing security consciousness training to the staffs.

#### ❖ **Recognizing and modifying third party risks-**

CISO must be aware about vendor supplied appliances especially for the software, organization procured in the period of emergency. Lots of secondary sources suggests that it is one of the vital way hackers send malicious software to the organization and take control upon the server.

❖ **Ensuring Cyber Safety within Institutional Code-**

It is essential to examine the new code and revisit other codes which are already installed in the systems to uproot any vulnerability or bugs. Experts suggest getting cyber safety code from local developer instead of receiving it from foreign countries

❖ **Built own software and application-**

The countries that are standing in the top position in terms of the Cyber security index all built their own application software to run critical infrastructure. Discouraging government enterprise to purchase Commercial off-shelf software (COTS) applications software

Most of the case COTS application attract the attackers as the product are well-known and available as beta version in community to test the bug. The COTS application always builds in concern of services and functionality rather than security point of view. Embedded malware, design or coding flaws exposing software even if code signing done and its doesn't provide any kind of assurance from vulnerabilities if we have secured infrastructure too. Disclosure of sensitive data after installation of application meaning we are procuring code and installing it in our secure infrastructure but later there are possibilities that application starts sending data to the vendor meaning unauthorized backdoor mechanisms could be implemented. we don't have knowledge/visibility of source code of the application and only can test functionality of the application. Vendors has limited liability in concerns of any losses happened due to any incidental consequences and damages including loss in business, revenue, profit and reputation. Considering the risk of COTS application, we need to incorporate some specific requirements to safeguard the application by considering security as a part of application purchasing process and that will build our confidence to select right vendor while acquiring the application. Establishment of compliance with security metrics and SLA which will liable vendor in future if any incident occurred.

Visibility of different components of the application with there's integration.

Ensure black box testing with DAST (Dynamic Applications Security Testing) and negative testing (Negative testing makes sure that your application can manage unexpected user behavior or invalid input with grace) done and evaluated by third



party with relevant certification for validity check. And the vendor has followed industry standard control framework while developing the application E.g. ISO, CMMI L5, OWASP secure coding practices

❖ **Protecting against Ransomware Incidents-**

According to NCSI, in Bangladesh Ransomware occurrences hit second position in 2020 among other available cyber-attacks. CISOs are now on high alert about Ransomware attack. Penetration test and data backup on regular basis could be the simple way to get rid of such problem. To protect their computer networks from ransomware infection, the following recommendations can be followed as preventive measures:

a) Use a data backup and recovery plan for all critical data. Regular backups should be performed and tested to reduce the impact of data or system loss and to expedite the recovery process. It should be noted that network-connected backups can also be infected by ransomware; for maximum protection, critical backups should be isolated from the network.

b) Updating the operating system and software with the most recent patches. Most attacks target vulnerable applications and operating systems. Making certain that these are patched with the most recent updates significantly reduces the number of exploitable entry points available to an attacker.

c) Keep anti-virus software up to date, and scan all software downloaded from the internet before running it.

d) Limit users apply to the "Least Privilege" approach to all systems and services and have the authority to install and run undesirable software programs. By restricting certain rights, malware may not be allowed to operate or spread widely over the network.

e) Allowing macros from email attachments should be avoided. If a user opens the attachment and enables macros, embedded code on the machine will execute the malware.

f) Do not click on suspicious emails Links.

❖ **Receiving Top Administrative Level Support-**

All executive level officers in an organization should be aware of existing information threat landscape and how much extra investment is needed to tackle them. CISO will present it directly to the board of executives meeting and alert them with its consequences.

❖ **Backing for Change Management and Strategic goals-**

As institutions endure to digitalize and quicken their changes, CISOs are expected to keep pace. Therefore, CISOs are thoughtful about safety as a business enabler. In order to protect employees, service seekers and the enterprise overall and new changes and strategic goals will be supported by top management.

❖ **Snowballing Agility-**

CISOs should be training themselves and their team members to work in a more agile mode to keep up with the business even in pandemic situations. Short comings may come up in any time any situation.

❖ **Upskilling the Organizational Squads-**

Rivalry for security ability is aggressive, with the pandemic intensifying an already viable market. CISOs remain to highlight keeping their present workforces and training them for the particular skills they need to safe sprouting situations. There's a specific priority on upskilling employees in cloud security and threat intelligence as well as access and identity management.

❖ **Addressing IoT Security-**

IoT experts in its *State of the IoT 2020* statement projected that there were 12 billion Internet of Things (IoT) networks last year, a number that for the first time exceeded the number of non-IoT links. There would be more than 30 billion IoT connections by

2025. CISOs have been giving much attention to the security around linked devices and the data they originate. They're formulating policies to know precisely what and how much they have linking to their system. They're also reexamining their uniqueness and access management programs to include IoT.

The security vulnerabilities and dangers covered in this essay cannot be resolved quickly. To adequately protect the Internet of Things' more specialized systems and components, particular procedures and technologies could be needed. However, by adhering to a few recommended practices, users can lower risks and stop threats:

a) Decide on who will administer things. IoT device and network administrators can lessen security lapses and vulnerabilities by managing IoT devices and the network. They will be in responsible of making sure that IoT devices, even those at home, are secure. The position is crucial, particularly in the WFH era, since IT professionals have little control over protecting home networks, which are now more influential on business networks.

b) Regularly check for patches and updates. In the IoT space, vulnerabilities are a significant and ongoing worry. This is as a result of the fact that any layer of IoT devices can have vulnerabilities. Cybercriminals continue to infect devices using outdated vulnerabilities, showing how long unpatched devices can stay online.

c) For all accounts, use strong and unique passwords. Strong passwords aid in the prevention of many cyberattacks. Password managers can assist users in creating unique and secure passwords that can be stored in the app or software itself.

d) Give importance to Wi-Fi security. Users can achieve this by turning on the router firewall, disabling WPS, turning on the WPA2 security protocol, and employing a secure Wi-Fi password. The secure router settings are another aspect of this process.

e) Keep an eye on baseline network and device behavior. Cyberattacks are notoriously difficult to detect. Knowing the baseline behavior of devices and

networks (speed, typical bandwidth, etc.) can help users spot deviations that indicate malware infections.

f) Segment the network to your advantage. By creating two networks—one for IoT devices and another for guest connections—users can lower their vulnerability to IoT-related assaults. Additionally, network segmentation helps isolate potentially problematic devices that cannot be taken offline immediately and stop the spread of assaults.

g) Secure the network and use it to improve security. IoT devices can put networks at risk, but networks can also act as a level playing field for users to implement security measures that cover all connected devices.

h) Protect IoT-cloud convergence and implement cloud-based solutions. The Internet of Things and the cloud are becoming increasingly intertwined. It is critical to consider the security implications of each technology in relation to the others. Cloud-based solutions can also be considered to provide IoT edge devices with additional security and processing capabilities.

i) Think about security solutions and tools. The limited capacity with which users can implement these steps is a significant barrier that users face when attempting to secure their IoT ecosystems. Certain device configurations could be restricted and challenging. Users can augment their efforts in these situations by thinking about security solutions that offer endpoint encryption and multi-layered protection.

j) Consider the various protocols employed by IoT devices. IoT devices communicate using not only internet protocols, but also a diverse set of networking protocols. To reduce risks and prevent threats, administrators must understand the entire set of protocols used in their IoT systems.

k) Protect the extensive use of GPS. Some IoT devices and applications heavily rely on GPS, which raises security concerns. Particularly if they employ positioning systems for manufacturing, monitoring, and other uses,

organizations should be careful of instances where GPS signals are jammed or even spoofed. If these positioning systems are critical to a business, the company should also have a way to monitor the GPS signal. Another option is for the company to use additional positioning systems.

Aside from implementing these security practices, users should also be aware of new technological developments. In recent years, there has been a greater emphasis placed on IoT security. Research on how to secure specific industries, monitor IoT-related threats, and prepare for upcoming gamechangers such as 5G is ongoing. Users must understand that the Internet of Things is an active and evolving field, and that its security must constantly transform and adapt to its changes.

❖ **Safekeeping by design-**

Consider everything e.g., products and services for our customers or tools and technologies that enable our employee experience—all must be embedded proper security, confidentiality, faith and compliance from the beginning.

❖ **Further Automation-**

Security automation has now become a very significant aspect of handling security incidents. CISOs are using automation to well identify threats and rapidity reaction as well as impose security principles throughout the improvement and placement of new code into the setting. Automation is a crucial portion of building secure code, executing security by design, and affecting to the progressively popular Zero trust security model.

Modern cyberattacks are highly automated. When organizations attempt to defend against these attacks manually, the battle becomes one of man versus machine, with the organization facing extremely unfavorable odds. It is essential to combat machine with machine, or, in this case, fire with fire, by introducing automation into cybersecurity operations in order to successfully defend against automated attacks. Automation creates a level playing field, lowers the number of threats, and speeds up the identification and avoidance of previously unidentified risks. Many security vendors believe that automation can increase productivity and reduce the need for additional staff members. While this is true, automation should also be seen as a tool

that may and ought to be used to more accurately anticipate behaviors and swiftly implement security measures. Automation can aid in the prevention of successful cyberattacks when utilized properly and with the appropriate tools. The following are some examples of how automation can be used:

a) Data Correlation. Massive volumes of threat data are gathered by numerous security firms. On the other hand, data isn't very useful until it is arranged into next steps that can be taken. Organizations must first gather threat data from all attack vectors, security technologies, and sources outside of their own infrastructure in order to do this efficiently. To predict the attacker's next action, they must first find groupings of threats that behave similarly among enormous volumes of data. By collecting more data, this strategy yields more precise answers and lessens the likelihood that the groups will spot an abnormality. As a result, the study needs to be able to scale the volume of threats that exist today, which cannot be done manually. Automation and machine learning make data sequencing quicker, more efficient, and more precise. Finally, this strategy combined with dynamic threat analysis is the sole way to identify sophisticated and previously unidentified threats.

b) Building up defenses more quickly than an attack can spread. Protections must be created and disseminated as soon as feasible when a danger has been identified to prevent an attack from spreading across the organization's networks, endpoints, or cloud. The optimum spot to stop a newly discovered assault is not where it was detected, but at the attack's anticipated next stage, due to the time penalty imposed by analysis. When coordinating different security vendors in the organization's environment and lacking the necessary control and resources, manually developing a full set of protections for the various security technologies and enforcement points capable of countering future behaviors is a time-consuming process. Defense development can be accelerated by automation without depleting resources.

c) Establishing defenses more quickly than assaults can spread. Protections must be put into place after they have been created in order to stop the attack from continuing at that stage in its lifecycle. Protections should be applied not only in the area where the threat was discovered but also across other technologies within the company in order to offer consistent defense against

the attack's present and potential future behaviors. Automation in the dispersion of defenses is the only method to outpace an automated and well-planned attack and stop it. With automated, big data attack-sequencing and automated production and dissemination of defenses, organizations can more correctly predict the next stage of an unknown assault and act swiftly enough to avoid it.

d) Identifying Current Network Infections, A timer starts counting down from the moment a threat enters the network until it results in a breach. To stop an attack before data leaves the network, authorities must act more quickly than the attack itself. In order to locate an infected host or spot suspicious activity, authorities must be able to examine data from their environment both backward and forward in time. Like analyzing unknown threats trying to infiltrate the network, it is challenging to scale manually correlating and analyzing data across their network, endpoints, and clouds. Automation offers quicker analysis as well as quicker identification and intervention in the event that a host on their network is compromised.

Automation is used by attackers to move quickly and deploy new threats at breakneck speeds. Automation as part of an organization's cybersecurity efforts is the only way to keep up with and defend against these threats efficiently. A next-generation security platform analyzes data quickly, converting unknown threats into known threats, creating an attack DNA, and automatically creating and enforcing a full set of protections across the organization to stop the attack lifecycle. Most organizations cannot, and should not, automate everything at once. Start off where security automation makes the most sense or can offer the quickest return on investment. The firm can monitor its progress, think the outcomes, make necessary adjustments, and then utilize that information as it expands automation into new areas by implementing it gradually.

To ensure that the security team follows a consistent and repeatable procedure each time an incident happens, it is crucial to document the processes, instructions, and best practices for effectively resolving problems. Staff must be properly trained to use security automation software, but they must also be trained to handle complicated occurrences that the software is unable to handle. When alerts are flagged as requiring

human invention, the organizational staff must be knowledgeable and confident in dealing with the issues.

#### ❖ **Strengthening Remote work Security-**

CISOs have a belief that out-of-the-way work has made their institutions further vulnerable to cyberattacks. They see more targeted occurrences since facilitating widespread remote work. Therefore, CISOs endorsing zero trust and identity-first security strategies to generate a protected work-from-anywhere business model, according to predictors, academics, and mentors. Because remote and hybrid work environments are here to stay, CISOs must develop an effective security strategy to manage the expanding attack surface. As ransomware cases and demands continue to rise, organizations can no longer afford (quite literally) to play catch-up with remote work security. Here are three long-term ways for organizations to strengthen their remote work security posture:

- a) Improving endpoint management. Threat actors do not limit themselves to a single silo such as endpoints and instead use additional channels in the same attack, such as email, network, and SaaS, despite the limited technologies such as endpoint detection and response being useful. By implementing a platform with enhanced detection and response capabilities that gathers and correlates data from all endpoints and security layers, giving security professionals the complete picture, they need to decrease mean time to detect/respond, they may achieve comprehensive visibility. The capacity to precisely identify what and who is present in their network is another part of good endpoint security. The Zero Trust strategy—which starts with the premise that every device, user, or program is dishonest, weak, or compromised—comes into play in this situation. While limited technology such as endpoint detection and response can be useful, threat actors do not confine themselves to a single silo such as endpoints and instead employ other channels in the same attack such as email, network, and SaaS. They can achieve comprehensive visibility by deploying a platform with extended detection and response capabilities that collects



and correlates data from all endpoints and security layers, providing the complete picture security teams require to reduce mean time to detect/respond. Another aspect of effective endpoint security is the ability to clearly identify what and who is in their network. This is where the Zero Trust approach—the assumption that any device, user, or app is untrustworthy, vulnerable, or has been compromised—comes into play. By scanning and authenticating users, devices, and apps before granting them network access, you reduce the possibility of a malicious user gaining and maintaining residence. Remember to keep an eye on network endpoints for any compromises or unusual behavior.

b) Inform employees about social engineering. Documenting CISO policies should include educational resources and regular social engineering testing. Baiting, phishing, spear phishing, and pretexting are all examples of social engineering. These attacks are used to gain access to sensitive data and are more common during high-profile events and when an employee is on the road. Assuring that the teams understand what to look for so that they can report any threats that come their way. Many businesses have found success in simulating these attacks and using them as an additional training and testing resource for employees.

c) Two-factor authentication. Employees benefit from an additional layer of security when using multi-factor authentication. Even if passwords or credentials are compromised, multi-factor authentication will help prevent attackers from gaining access to the organization.

d) Making use of VPN connections. Though VPN is not widely used in government organizations, it is hoped that it will become a part of their security posture in the near future. Employees can use Virtual Private Networks to securely transfer files and share data even when using a public WIFI network. VPNs, on the other hand, are useless if employees do not use them. Make a point of emphasizing the importance of VPNs in their security documentation.

e) Reconfigure your WiFi password. Because everyone works from home, there's a chance that neighbors, friends, and others have accessed the employee's WIFI network. Encourage employees to change their WiFi passwords on a regular basis in case there are any unauthorized users on the network.

f) Regularly install updates. Ensure that employees, even if they are remote, are installing software updates on a regular basis. These updates frequently include critical security patches that no one wants to be without. Larger updates should be distributed via email to ensure that employees not only install but also correctly install these updates.

Many people are now working from home for the first time as a result of the COVID-19 outbreak. With this new reality, businesses must take extra security precautions to ensure that such a drastic operational shift does not introduce new security risks into their operations.

#### ❖ **Safeguarding the Cloud-**

Many organizations augmented their public cloud use during the pandemic, with most of them signifying the shift to public cloud would be permanent. Those institutions deployed fresh tools, processes, and control models to support the infrastructure. CISOs executing comprehensive cloud security control program to get their team prominence into enterprise's cloud environment and to impose loyalty to appropriate arrangements and security controls. Cloud security is a collection of procedures, policies, and technologies that work together to safeguard data, applications, and systems hosted in the cloud. Because every business has millions of records stored in the cloud, cloud computing security is critical.

Cloud security is a new level of difficulty for CISOs. They must make numerous efforts to protect their data or applications from malicious actors while also continuing to operate. We have compiled a list of top tips to assist CISOs in managing their organization's cloud security. These tips, if carefully implemented, can work

wonders for cloud security, whether it's Azure security or Google Cloud Security. CISOs can use the following guidelines to address the cloud security issue:

a) Work with the organization to strategically deploy cloud security. CISO security should look for a company that thoroughly analyzes its cloud requirements and develops a comprehensive cloud computing security strategy. Many organizations are taking this seriously and have already begun redesigning and collaborating with teams that combine security and IT with shared KPIs. This method is known as "security by design," in which a proper architecture is designed and then strategically implemented by experts.

b) Identify data flows. When we talk about data flows, we're referring to the movement of data in the cloud. It is critical for CISO security to understand their organization's data flows. The main reason for this is that if they understand the flow, they will be able to identify any loopholes that may exist. It also aids them in risk assessment.

c) Implement the best API security. The cloud has made it simple for businesses to access their supply chain risks. It is related to the previous point about determining data flows, but it also goes ahead. More opportunities will arise as the CISO integrates the cloud into the organization. As a result, the CISO must have security protocols built on cloud APIs to prevent unauthorized access. They will empower the organization's cloud while lowering the risk of a breach.

d) Set up zero-trust network access. It is something that CISO security should think about, which means that you should no longer grant access to any device or cloud service without authenticated security credentials. This solution will raise the organization's cloud security or Azure security to a new level, and it will be useful if the CISO is about to enter the cloud world.

e) Risk awareness and workforce activation Everyone is concerned about information security in the cloud. However, while working on security, we must also be aware of the risks and threats that may emerge unexpectedly.

Because it only takes one simple error to bring the entire system down, the CISO should keep a close eye on the organization's system. Activating the workforce is the most effective solution for this. Creating a cloud workforce will assist the CISO in preventing even the organization's employees from accessing unauthorized areas of the cloud. And trust us when we say that this will protect the organization's cloud from internal breaches.

Because the cloud is a revolution in IT architectures, cost centers, and workflows, it must be secure when implemented into an organization's business. As CISO, it is your responsibility to take every security precaution to keep your organization's data safe in the cloud. We hope that these tips will assist the CISO in keeping the organization's cloud secure and instilling a positive workforce mindset within the organization. When data is stored in a potentially unsafe environment, organizations tend to migrate to the cloud. As a result, the guidelines can be followed to improve cloud security and data integrity.

The key to ensuring that organizations have the greatest possible success is to encourage employees to develop good cybersecurity habits. Employees should have a clear understanding of and commitment to cybersecurity. It is less likely that staff will communicate on non-secure platforms or store critical data in non-secure online spaces when it is culturally ingrained.

❖ **Carry on with emerging, evolving privacy laws-**

Bangladesh Government has already drafted Data Protection Act 2020. Such actions are produced an increasing patchwork of privacy protocols that institutions must abide and follow. It is almost a daily discussion with CISOs and corporate leaders.

Even if a company believes it is compliant, regulations are constantly changing, necessitating the implementation of new data privacy efforts. It is difficult to stay in compliance with the ever-changing requirements of global privacy regulation. Organizations must not only assess, develop, and monitor your privacy compliance program, but they must also be prepared to adapt as needed. Given the changes in the political and legal landscape, here are a few ways for organizations to assess their exposure and begin developing a plan of action:

- a) Make a list of all the personal information in their environment.
- b) Determine how their current process involves the collection, use, sale, and distribution of that information.
- c) Determine any discrepancies between existing processes and applicable regulatory requirements.
- d) Create and maintain a privacy compliance program.

❖ **Formulating Business Continuity Plan and national cyber security strategy-**

In order to respond to disruptions of business activities arise from main catastrophe of information systems or disasters and to confirm the timely reopening of actions, a business continuity controlling procedure should be realized. Through a combination of protective and regaining controls, it is important to reduce the impact of disaster on the institution and to recover from damage to information assets (which may be caused by, for example, natural disasters, accidents, equipment failures, and deliberate actions) at a tolerable level.

Cyber security Contingency planning and strategy **for public information infrastructure should be ready.** Information systems are susceptible to a wide range of disruptions, from minor (such as a brief power outage or disk drive failure) to major (such as equipment destruction, fire, or cyberattack), which can be caused by either natural or man-made catastrophes. In 2021, cyberattacks dominated the news as severe disruptions hit the nation's federal agencies. As part of the organization's resilience strategy, much vulnerability may be reduced or removed through management, operational, or technical controls; nonetheless, it is practically difficult to eliminate all risks. By offering practical and cost-effective ways to improve system availability, contingency planning aims to reduce the risk of system and service unavailability.

Business continuity entails keeping an organization's operations running in the face of disruptions such as natural disasters, pandemics, cyber-attacks, and other technical issues, among others. To provide services to its citizens, government organizations must always be operational. Of course, each organization has its own distinct operations and practices, and these characteristics influence the organization's specific business continuity plan. However, in the digital age, all organizations have an online

presence, which means cybersecurity concerns must be incorporated into their continuity plan.

Every time an organization's network or servers go down, their operations suffer a disruption in business continuity, which can result in painful consequences and criticism. Cyber security risks evolve quickly, and business continuity plans must evolve in tandem to ensure that they remain useful. With such rapid changes, however, misconceptions and myths about business continuity planning may stymie their path to success. Before developing the best continuity plan for their business operations, organizations must be wary of these common misconceptions. Organizations must recognize that business continuity planning cannot exist as a separate business process from the rest of their operations, particularly cybersecurity. Cybersecurity must be a critical component of their business continuity plans.

A cybersecurity attack could cause downtime, triggering their business continuity plan, or any type of business operation disruption could make the systems particularly vulnerable to cyber risks. This relationship is recognized by an effective continuity strategy.

Public enterprise running critical infrastructure should Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in place and routine exercise of BCP/DRP. The Government should make a national cyber security Contingency Plan and guideline.

### **8.3 Implications**

This research knowledge will add value to the university researcher, criminal judges, security forces, IT personnel and legislative bodies, owners of CII, lawmakers, IT end users from the Government and the Non-government organization (together with financial institutes), telephone enterprises and the banking division.

### **8.4 Indication for Future Research**

This research holistically engaged three information security domains to scrutinize ISG correlates to Bangladesh government sector. Though interagency ISG professional sector undoubtedly significant here, it may be necessary to reimburse

ISG efficiency at the employee level because any single method to an ISG execution approach and formulated tactics doesn't confirm successful recognition (Silic & Back, 2014 and Yaokumah, 2013). Therefore, further research should undertake in order to achieve ISG proficiency in businesses within upcoming threats and vulnerabilities.

The findings and recommendations might not be valid for all other types of government organizations in Bangladesh, especially if the institutions are not similar in terms of environmental, organizational, and internal structure. Forthcoming researchers may embrace another suitable method to unveil certain phenomena related to ISMS. New potential methods to be used in an integrative triangulation approach or combining both quantitative and qualitative design involving in-depth interviews with top-level managers of the government organization. Moreover, there are other likely areas to be explored such as the national strategy, regulation, and other external influences in organizational ISMS.

This work has got some limitations. The number of respondents was not fairly big for an interview on ISG surveys. Forthcoming academics may follow ISG exploration using a vast sample size with advanced research procedures that produce elaborate response to validate the offered model. Instead, Barton (2014) suggested that imminent scholars deliberately substituting self-reported IS assessments with a researcher or arbitrator valuations.

There is only a few or no study had specifically conducted to assess the readiness of Bangladesh Government organizations' ISG executions. Prospect researchers will comprehend existing theoretical literature allowing possible tactical developments needed to almost confirm deterrence and prevention of IS threats.

#### **8.4.1 Future Scope**

The aim of this study is to identify the most significant information dangers, threats, and vulnerabilities that typically occur in some key Bangladeshi Government leading organizations. As the research mainly focuses on government organizations because the national database of public data resides in such organizations. The future scope of the following research can be conducting the research considering the Information Security for the non-government organizations as well. Therefore, the future scope of this research contains both the government and non-government organizations as a

society requiring several implementations of security levels for persevering Information Security for the critical, confidential, and important data.

## **8.5 Objective fulfillment**

- This research has determined the most important information risks, threats, and vulnerabilities that frequently occur in some key Bangladeshi government leadership organizations (such as the Bangladesh Bank, Election Commission, CID/SB of the Bangladesh Police, Land Records and Survey Department, etc.).
- It has given a thorough grasp of the unintended effects and repercussions of various information risks in public companies or organizations, as well as the protective measures that the organizations take against threat attacks. the type of attack, its frequency, and a target analysis.
- The research has assessed the efficacy of the current protection mechanisms implemented in those significant Bangladesh Government leading organizations by examining their result rate and conducting interviews.
- The research has provided new insights into the best practices appropriate to handle these incidents in a very efficient manner, analyzing the threat patterns and reports for potential future attack management in a sufficient manner.

## **8.6 Conclusion**

Cyber risks are blooming and remodeling rapidly. Network hackers are always engaged in new methodologies for capturing the IT security systems of establishments. While doing this, they jeopardize the system by accessing into sensitive data and theft scholarly resources. Generally, the information incidents have become more sophisticated and difficult to prevent. It is due to continuous evolution; we are unable to imagine what types of threats are ahead. It could only guess that those threats could be even much threatening than the present ones. It is also certain that as old sources of cyber threat fade, new sources will emerge to take their place. Despite this insecurity, organizations need to be sanguine about the nature of cybersecurity they really need.

To get information security right in place, initially we must get a solid foundation of IT in the organization. Although recently much responsiveness has been given to



cyber incidents, IT users now know the consequential hazards. There might be few reasons for some government offices that are still not launching elementary processes and Information systems security in place. Once the basis has been installed, the following steps are upgraded, organization's information security will more vibrant and synchronized with and incorporated into main business continuity strategy. Without implementing this crucial phase, organizations persist in susceptible — especially when the office settings and the information threats & vulnerabilities they encounter are all shifting. And then arise the actual opportunity: the chance to get one-step ahead of cyber criminals. By concentrating on Information security for the beginners — the future and business's broader ecosystem — we can start building cyber capabilities before they are needed and initiate preparation for threats before they again get up.

Organizations must look forward and behind the businesses as new vulnerabilities and threats are being formed today and we require staying ahead of the situation. Although a good number of studies do not suggest that hackers will get there soon, we should be more proactive and advance knowledge about information security to become the culture of every organization. We want the effort to be on increasing the cyber capacity of the organization because businesses have grasped the foundation; Intruders are using cutting-edge new strategies and always employing dominant new tools, making them more powerful and safe than ever. We want businesses to lead the way in making cybercrime much less profitable and a more passive use of time and resources than it is right now. In other words, eliminate the hacker's power to combat cybercrime.

## References-

Aspire to Innovate (A2I) Program, (2011). Strategic Priorities of Digital Bangladesh. Dhaka: Government of Bangladesh, p.265.

Aspire to Innovate (A2I) Program, (2014). *e-Tathyakosh: Enhancing Access to Livelihood Information*. Dhaka: Government of Bangladesh, p.2.

Aspire to Innovate (A2I) Program, (2016). A TCV + Study on National Portal Service. Dhaka: Government of Bangladesh, p.23.

Aspire to Innovate (A2I) Program, (2018). Union Digital Centers: Reaching the Unreached through an Innovative Public Private Entrepreneurship Model. Dhaka: Government of Bangladesh, p.4.

Aspire to Innovate (A2I) Program, (2019). Honorable ICT Affairs Adviser to HPM Launched ekSheba, ekPay and ekShop. Dhaka: Government of Bangladesh.

a2i. 2020. About - a2i. [online] Available at: <<https://a2i.gov.bd/about/>>.

Ahmad, T. (2021). E-Government in Bangladesh: Development and Present State. International Journal of Social Science and Human Research, 04(01). doi:10.47191/ijsshr/v4-i1-15.

AlGhamdi, S., Win, A/Prof.K.T. and Vlahu-Gjorgievska, Dr.E. (2020). Information Security Governance Challenges and Critical Success Factors: Systematic Review. Computers & Security, p.102030. doi: 10.1016/j.cose.2020.102030.

Andrew Barton, K., (2014). Information System Security Commitment: A Study of External Influences on Senior Management. Ph.D. Nova Southeastern University.

Arbanas, K., Spremic, M. and Zajdela Hrustek, N., (2021). Holistic framework for evaluating and improving information security culture. Aslib Journal of Information Management, 73(5), pp.699-719.

Bangladesh Police, (2019). Anti-Terrorism Unit, Bangladesh Police. (n.d.). ICT Policy. Dhaka: Government of Bangladesh.

Bb.org.bd. (2015). Guideline on ICT Security for Banks and Non-Bank Financial Institutions. [online] Available at: <[https://www.bb.org.bd/aboutus/regulationguideline/brpd/guideline\\_v3\\_ict.pdf](https://www.bb.org.bd/aboutus/regulationguideline/brpd/guideline_v3_ict.pdf)>.

Bb.org.bd. (2019). Bangladesh Bank. [online] Available at: <<https://www.bb.org.bd/en/>>

Bangladesh Gazette (Additional Issue). (2014). Information Security Policy Guideline. Information and Communication Technology Division, Agargaon, Dhaka. Available at: <<https://icb.portal.gov.bd> > [icb.portal.gov.bd](https://icb.portal.gov.bd) >.

Baskerville, R. and Siponen, M., (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), pp.337-346.

BBC (2000). BBC - Homepage. [online] Bbc.com. Available at: <https://www.bbc.com/>.

Bhattacharjee, A., (2022). *Social Science Research: Principles, Methods, and Practices*. [online] Digital Commons @ University of South Florida. Available at: <[https://digitalcommons.usf.edu/oa\\_textbooks/3/](https://digitalcommons.usf.edu/oa_textbooks/3/)>.

Brewerton, P and Millward, L (2004). *Organizational Research Methods: A guide for students and researchers*. Thousand Oaks, CA: Sage Publications, Inc. Available at: <<https://www.semanticscholar.org>>.

Brutus, S., Aguinis, H. and Wassmer, U., (2012). Self-Reported Limitations and Future Directions in Scholarly Reports. *Journal of Management*, 39(1), pp.48-75.

Calder, A. (2014). *Cyber Essentials: A Pocket Guide*. IT Governance Ltd. Available at: <<https://books.google.com.bd/books>>

Chaula, J. (2006). *A Socio-technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance*. undefined. [online] Available at: <https://www.semanticscholar.org/paper/A-Socio-technical-Analysis-of-Information-Systems-%3A-Chaula/af1396672aa969a9db68713637618d8278dd0c44>.

Chan, H. and Mubarak, S. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications*, [online]

60(10), pp.23–31. Available at:  
<https://www.ijcaonline.org/archives/volume60/number10/9729-4202>.

Chen, Y.N., Chen, H.M., Huang, W. and Ching, R.K.H. (2006). E-Government Strategies in Developed and Developing Countries. *Journal of Global Information Management*, 14(1), pp.23–46. doi:10.4018/jgim.2006010102.

Choobineh, J., Dhillon, G., Grimaila, M.R. and Rees, J. (2007). Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems*, [online] 20. doi:10.17705/1cais.02057.

CICA, R.E.D.M.C. (2012). *Assuring Information Security*. 1st edition ed. [online] Amazon. Robert E. Davis. Available at: <https://www.amazon.com/Assuring-Information-Security-Assurance-Services-ebook/dp/B008CKIIW2>.

CID | Bangladesh Police. [online] Available at: <https://www.cid.gov.bd/>.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, [online] 14(4), pp.186–196. Available at:  
<https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/Previous%20Articles/Ch11InternalThreatsUsers.pdf>.

Cost of Data Breach Study: (2021) Japan Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. (2012). [online] Available at: [https://www.ponemon.org/local/upload/file/2011\\_%20CODB\\_JP\\_Final\\_5.pdf](https://www.ponemon.org/local/upload/file/2011_%20CODB_JP_Final_5.pdf)

Dalal, A.K. (1999). Book Reviews: Carol Grbich, *Qualitative Research in Health: An Introduction*. London: Sage Publications, 1999, pp. 312. £47.50 (hb), £15.99 (pb). *Journal of Health Management*, 1(2), pp.367–371. doi:10.1177/097206349900100213.

Dan-Suteu, Stefan-Antonio. (2018). Boosting Cyber Security Innovation and Culture through Public-Private Research Projects. 10.12753/2066-026X-18-217. Available at: [https://www.researchgate.net/publication/331968542\\_Boosting\\_Cyber\\_Security\\_Innovation\\_and\\_Culture\\_through\\_Public-Private\\_Research\\_Projects](https://www.researchgate.net/publication/331968542_Boosting_Cyber_Security_Innovation_and_Culture_through_Public-Private_Research_Projects).

Da Veiga, A. and Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), pp.243–256. doi: 10.1016/j.clsr.2015.01.005.

Denscombe, M. 2013 The role of research proposals in business and management education. *The International Journal of Management Education*, 11, 142-149. doi: 10.1016/j.ijme.2013.03.001

Detert J, Schroeder R, Mauriel J. 2000 A framework for linking culture and improvement initiatives in organizations. *The Academy of Management Review* 2000; 25(4):850–63.

Developer, M.A.M.I.K.L.N.S.W.D.S.A.D.J.H. (n.d.). Bangladesh to automate land management and services, says official document. [online] unb.com.bd. Available at: <https://unb.com.bd/category/Special/bangladesh-to-automate-land-management-and-services-says-official-document/77754>.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, [online] 11(2), pp.127–153. doi:10.1046/j.1365-2575.2001.00099. x.

Dhillon, G., Syed, R. and Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, 56, pp.63–69. doi: 10.1016/j.cose.2015.10.001.

Dhiman, V.D. (2022). Importance of Information and Communication Technology (ICT) in Higher Education Paper. In: *International Conference on Computing, Communication, Electrical and Biomedical Systems*. Switzerland: Springer International Publishing.

Dimaggio, P. (1988). Interest and agency in institutional theory. *Research on Institutional Patterns: Environment and Culture*. [online] Available at: <https://nyuscholars.nyu.edu/en/publications/interest-and-agency-in-institutional-theory>.

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009). Information security: the moving target. *researchspace.csir.co.za*. [online] Available at: <https://researchspace.csir.co.za/dspace/handle/10204/4649>.

Dong, K., Ali, R.F., Dominic, P.D.D. and Ali, S.E.A. (2021). The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainability*, 13(5), p.2800.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1), pp.67–87. doi:10.2307/41166154.

Eloff, J. and Eloff, M. (2003). Information security management: a new paradigm. undefined. [online] Available at: <https://www.semanticscholar.org/paper/Information-security-management%3A-a-new-paradigm-Eloff-Eloff/1a102731e0807269a0dc23483e3f6bf3acfc80ee>.

Ernst & Young (E&Y). (2009). Outpacing change. (n.d.). [online] Available at: <https://www.equipoitalento.com/contenido/download/estudios/GISS.pdf>.

Express, T.F. (n.d.). Police data centre project likely to get ECNEC approval. [online] The Financial Express. Available at: <https://thefinancialexpress.com.bd/national/police-data-centre-project-likely-to-get-ecnec-approval-1534171906>

Flores, W. R, Antonsen, E, & Ekstedt, M. 2014 Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110. doi: 10.1016/j.cose.2014.03.004

Gehem M, Usanov A, Frinking E & Rademeker M. 2015 Assessing Cyber Security: A Meta-Analysis of Threats, Trends and Response of Cyber Attacks. The Hague Center for Strategic Studies (HCSS), The Netherlands. Available at: [https://www.researchgate.net/publication/319677972\\_Assessing\\_Cyber\\_Security\\_A\\_Meta-analysis\\_of\\_Threats\\_Trends\\_and\\_Responses\\_to\\_Cyber\\_Attacks](https://www.researchgate.net/publication/319677972_Assessing_Cyber_Security_A_Meta-analysis_of_Threats_Trends_and_Responses_to_Cyber_Attacks)

Guidance for Information Security Managers. (n.d.). [online] Available at: <http://www.csun.edu/~yz73352/657/sent-0710/InfoSec-Guidance-for-Mgrs-Research-21May08.pdf>.

Gupta, M & Raj, S. 2009 Handbook of Research on Social and Organizational Liabilities in Information Security. London: IGI Global. Available at: [https://www.researchgate.net/publication/267562515\\_Handbook\\_of\\_Research\\_on\\_Social\\_and\\_Organizational\\_Liabilities\\_in\\_Information\\_Security](https://www.researchgate.net/publication/267562515_Handbook_of_Research_on_Social_and_Organizational_Liabilities_in_Information_Security)

Haeussinger, Felix and Kranz, Johann, (2017). "ANTECEDENTS OF EMPLOYEES' INFORMATION SECURITY AWARENESS - REVIEW, SYNTHESIS, AND DIRECTIONS FOR FUTURE RESEARCH". In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017 (pp. - ). ISBN 978-989-20-7655-3 Research Papers.

Halim, H. and Mohd, M. (2019). Framework for Digital Data Access Control from Internal Threat in the Public Sector. International Journal of Advanced Computer Science and Applications, 10(8). doi:10.14569/ijacsa.2019.0100809.

Hayat, M.J. (2013). Understanding Sample Size Determination in Nursing Research. Western Journal of Nursing Research, 35(7), pp.943–956. doi:10.1177/0193945913482052.

Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan. 2011. Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05.

Hina, S. and Dominic, P.D.D. (2018). Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems, 60(3), pp.201–211. doi:10.1080/08874417.2018.1432996.

Hofstede, G. (2011). Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. [online] DigitalCommons@USU. Available at: [https://digitalcommons.usu.edu/unf\\_research/53/](https://digitalcommons.usu.edu/unf_research/53/).

Hu, Q, Dinev, T, Hart, P, & Cooke, D. 2012 Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43, 615-660.

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit - DuD*, [online] 35(1), p.7. Available at: [https://www.academia.edu/2242298/Information\\_security\\_management\\_system\\_standards\\_A\\_comparative\\_study\\_of\\_the\\_big\\_five](https://www.academia.edu/2242298/Information_security_management_system_standards_A_comparative_study_of_the_big_five).

Hsu, C., Wang, T. and Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. 2016 49th Hawaii International Conference on System Sciences (HICSS). doi:10.1109/hicss.2016.600.

IBIMA Publishing. (n.d.). Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review. [online] Available at: <https://ibimapublishing.com/articles/JIACS/2021/666987/>.

Ifinedo, P. (2014) Information Systems Security Policy Compliance An Empirical Study of the Effects of Socialization, Influence, and Cognition. *Information & Management*, 51, 69-79. - References - Scientific Research Publishing. [online] Available at: [https://www.scirp.org/\(S\(lz5mqp453ed%20snp55rrgjt55\)\)/reference/referencespapers.aspx?referenceid=2641691](https://www.scirp.org/(S(lz5mqp453ed%20snp55rrgjt55))/reference/referencespapers.aspx?referenceid=2641691).

Ivankova, N.V., Creswell, J.W. and Stick, S.L. (2006). Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Field Methods*, [online] 18(1), pp.3–20. doi:10.1177/1525822x05282260.

Jaeger 2013, J. (n.d.). Human Error, Not Hackers Cause Most Data Breaches. [online] *Compliance Week*. Available at: <https://www.complianceweek.com/human-error-not-hackers-cause-most-data-breaches/4048.article>.

Jaffe, R. and Cowell, J.M. (2014). Approaches for Improving Literature Review Methods. *The Journal of School Nursing*, 30(4), pp.236–239. doi:10.1177/1059840514540427.

Krishi Bank, B. (2014). INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY. [online] Available at: [https://www.krishibank.org.bd/wp-content/uploads/2016/09/ICT\\_security\\_policy\\_June\\_2014.pdf](https://www.krishibank.org.bd/wp-content/uploads/2016/09/ICT_security_policy_June_2014.pdf).



cirp.org. (2014). Board Briefing on IT Governance,” 2nd Edition, IT Governance Institute, 2009. - References - Scientific Research Publishing. [online] Available at: [https://www.scirp.org/\(S\(351jmbntvnsjt1aadkposzje\)\)/reference/ReferencesPapers.aspx?ReferenceID=1066940](https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1066940).

Khan, M.J. and Islam, S. (2018). New police unit to check cyber crime. [online] The Daily Star. Available at: <https://www.thedailystar.net/frontpage/new-police-unit-check-cyber-crime-1515997>.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021). Enhancing Employees Information Security Awareness in Private and Public Organizations: A Systematic Literature Review. *Computers & Security*, p.102267. doi: 10.1016/j.cose.2021.102267.

Khan, M.S. and Barua, S. (2010). The Status and Threats of Information Security in the Banking Sector of Bangladesh: Policies Required. [online] papers.ssrn.com. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1569207](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1569207).

Kitchin, R. (2013). *Conducting Research in Human Geography*. Routledge. doi:10.4324/9781315841458.

Knapp, K. (2005). A MODEL OF MANAGERIAL EFFECTIVENESS IN INFORMATION SECURITY: FROM GROUNDED THEORY TO EMPIRICAL TEST. [online] Available at: [https://etd.auburn.edu/bitstream/handle/10415/708/KNAPP\\_KENNETH.pdf?sequence=3](https://etd.auburn.edu/bitstream/handle/10415/708/KNAPP_KENNETH.pdf?sequence=3)

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013). Employees’ Information Security Awareness and Behavior: A Literature Review. [online] IEEE Xplore. doi:10.1109/HICSS.2013.192.

Lehto, M. and Neittaanmäki, P. eds., (2015). *Cyber Security: Analytics, Technology and Automation*. Intelligent Systems, Control and Automation: Science and Engineering. Cham: Springer International Publishing. doi:10.1007/978-3-319-18302-2.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International*

Journal of Information Management, [online] 45, pp.13–24. doi: 10.1016/j.ijinfomgt.2018.10.017.

Love, P., Reinhard, H., Schwab, A.J., & Spafford, G. 2010 Global Technology Audit Guide (GTAG) 15 Information Security Governance, Institute of Internal Auditors, USA.

Ma, Q. and Pearson, J.M. (2005). ISO 17799: ‘Best Practices’ in Information Security Management. Communications of the Association for Information Systems, 15. doi:10.17705/1cais.01532.

Maleh, Y., Sahid, A., Alazab, M. and Belaiassaoui, M. (2021). IT Governance and Information Security. doi:10.1201/9781003161998.

Managing for Enterprise Security. [online] Available at: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7019>.

Managing the Human Factor in Information Security: How to win over staff and influence business managers | Wiley. [online] Available at: <https://www.wiley.com/en-us/Managing+the+Human+Factor+in+Information+Security:+How+to+win+over+staff+and+influence+business+managers-p-9780470721995>

Manish, G. and Raj, S. (2008). Handbook of Research on Social and Organizational Liabilities in Information Security. [online] Google Books. IGI Global. Available at: <https://books.google.com.bd/books?id=PMbSXeHwBdgC&pg=PA510&lpg=PA510&dq=Cohen>.

Manuel, T. and Herron, T.L. (2020). An ethical perspective of business CSR and the COVID-19 pandemic. Society and Business Review, [online] p.-. Available at: <https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/en/covidwho-805463>.

McFadzean, E., Ezingard, J. and Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), pp.622–660. doi:10.1108/14684520710832333.

Mihal, R. and Zolotova, I. (2014). Incidents, alarms and events in information and control systems. 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). [online] Available at: [https://www.academia.edu/57112026/Incidents\\_alarms\\_and\\_events\\_in\\_information\\_and\\_control\\_systems](https://www.academia.edu/57112026/Incidents_alarms_and_events_in_information_and_control_systems)

Mohare, R. & Lanjewar, U. 2012. Determinants of business information security. International Journal of Marketing and Technology, 2(7), 203-209.

Nagin, D.S. (1998). Criminal Deterrence Research at the Outset of the Twenty-First Century. Crime and Justice, [online] 23, pp.1–42. Available at: <https://www.jstor.org/stable/1147539>.

Nahida Sultana, Md. Azharul Islam, Md. Mehedi Hasan and Md Mamun Rashid (2015). Report on ICT Policy in Bangladesh. Available at: [https://www.academia.edu/15235366/ICT\\_Policy\\_of\\_BD](https://www.academia.edu/15235366/ICT_Policy_of_BD)

Nasir, A., Arshah, R., Hamid, M. and Fahmy, S., (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, [online] 44, pp.12-22. Available at: <<https://www.sciencedirect.com/science/article/abs/pii/S2214212617306828>>.

Nasser, A., (2017). Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. [online] Research gate. Available at: <[https://www.researchgate.net/publication/325083796\\_Information\\_security\\_gap\\_analysis\\_based\\_on\\_ISO\\_27001\\_2013\\_standard\\_A\\_case\\_study\\_of\\_the\\_Yemeni\\_Academy\\_for\\_Graduate\\_Studies\\_Sana'a\\_Yemen](https://www.researchgate.net/publication/325083796_Information_security_gap_analysis_based_on_ISO_27001_2013_standard_A_case_study_of_the_Yemeni_Academy_for_Graduate_Studies_Sana'a_Yemen)>.

Nosworthy, J.D. (2000). Implementing Information Security in the 21st Century — Do You Have the Balancing Factors? Computers & Security, 19(4), pp.337–347. doi:10.1016/s0167-4048(00)04021-9.

www.oreilly.com. (n.d.). Information Security: The Complete Reference, Second Edition, 2nd Edition [Book]. [online] Available at: <https://www.oreilly.com/library/view/information-security-the/9780071784351/>

Pandit, N. (1996). The Creation of Theory: A Recent Application of the Grounded Theory Method. The Qualitative Report. doi:10.46743/2160-3715/1996.2054.

Police.gov.bd. (2014). Bangladesh Police. [online] Available at: <[https://www.police.gov.bd/en/police\\_cyber\\_support\\_for\\_women](https://www.police.gov.bd/en/police_cyber_support_for_women)>.

Posthumus, S. and Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), pp.638–646. doi: 10.1016/j.cose.2004.10.006.

IBM Security (2021). Cost of a Data Breach Report 2021. [online] Available at: <https://www.ibm.com/downloads/cas/OJDVQGRY>.

P.S, S., S, N. and M, S. (2018). Overview of Cyber Security. IJARCCCE, 7(11), pp.125–128. doi:10.17148/ijarccce.2018.71127.

Rajab, M. and Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Computers & Security, 80, pp.211–223. doi: 10.1016/j.cose.2018.09.016.

Raman, K & Wei, K 1992 The GDSS Research Report. In R.P. Bostrom, R.T. Watson & S.T. Kinney (Eds.). Computer Augmented Teamwork: A Guided Tour. Van Nostrand Reinhold: New York.

Rao, U. K. 2012 Concepts in sample size determination. Indian Journal of Dental Research, 23, 660-664

Rasheed, S., Wang, C.F. and Yaqub, F. (2015). Towards Program Risk Management and Perceived Risk Management Barriers. International Journal of Hybrid Information Technology, 8(5), pp.323–338. doi:10.14257/ijhit.2015.8.5.35.

Ravitch, M and Riggan, M. (2016). How Conceptual Framework Guide Research. The Qualitative Report, Fort Lauderdale, 21(9).

Ruighaver, A.B.P., (2022). 1 Exploring Organizational Security Culture: [online] Citeseerx.ist.psu.edu. Available at: <<https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.605.6589>>.

Safa, N.S., Solms, R. and Furnell, S. (2016). Information security policy compliance model in organizations. [online] undefined. Available at: <https://www.semanticscholar.org/paper/Information-security-policy-compliance-model-in-Safa-Solms/e40494ec05a43c652933d46f85435f0256450ab9>.

Schein, E.H. (2010). Organizational Culture and Leadership. 5th ed. Hoboken, New Jersey Wiley.

Schneberger, S & Wade, M. (2008). Socio-Technical System Theory. Available at: [http://www.fsc.yorku.ca/york/istheory/wiki/index.php/socio\\_technical\\_theory](http://www.fsc.yorku.ca/york/istheory/wiki/index.php/socio_technical_theory).

Schryen, G. (2013). Revisiting IS business value research: what we already know, what we still need to know, and how we can get there. European Journal of Information Systems, 22(2), pp.139–169. doi:10.1057/ejis.2012.45.

Sheth, A. (2021). RESEARCH PAPER ON CYBER SECURITY. [online] CONTEMPORARY RESEARCH IN INDIA. Available at: [https://www.researchgate.net/publication/352477690\\_Research\\_Paper\\_on\\_Cyber\\_Security](https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security).

Shivashankarappa, A.N., Smalov, L., Dharmalingam, R. and Anbazhagan, N. (2012). Implementing it governance using COBIT: A case study focusing on critical success factors. [online] IEEE Xplore. Available at: <https://ieeexplore.ieee.org/document/6280217>.

Shojaie, B., Federrath, H. and Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. 2015 10th International

Conference on Availability, Reliability and Security. [online] doi:10.1109/ARES.2015.25.

Silic, M. and Back, A. (2014). Information security. *Information Management & Computer Security*, 22(3), pp.279–308. doi:10.1108/imcs-05-2013-0041.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, 23(2), pp.200–217. doi:10.1108/ics-04-2014-0025.

Singh, M. and Mukhopadhyay, I. (2021). Cyber Security Issues in the COVID-19 Times. *Lecture Notes on Data Engineering and Communications Technologies*, [online] pp.671–680. Available at: <https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1188075>.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8), p.97. doi:10.1145/1145287.1145316.

Siponen, M. and Willison, R. (2007). A Critical Assessment of IS Security Research between 1990-2004. *ECIS 2007 Proceedings*. [online] Available at: <https://aisel.aisnet.org/ecis2007/190/>.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215–225. doi: 10.1016/j.ijinfomgt.2015.11.009.

Srnka, K.J. and Koeszegi, S.T. (2007). From Words to Numbers: How to Transform Qualitative Data into Meaningful Quantitative Results. *Schmalenbach Business Review*, [online] 59(1), pp.29–57. doi:10.1007/bf03396741.

Steiger, J.S., Hammou, K.A. and Galib, M.H. (2014). An Examination of the Influence of Organizational Structure Types and Management Levels on Knowledge Management Practices in Organizations. *International Journal of Business and Management*, [online] 9(6). doi:10.5539/ijbm.v9n6p43.

Straub, D., Goodman, S. and Baskerville, R. (2008). Framing the Information Security Process in Modern Society. *Information Security: Policy, Processes, and Practices*. [online] Available at: <https://espace.curtin.edu.au/handle/20.500.11937/33485>.

Team, B. e-GOV C. | B. e-Government C.I.R. (n.d.). BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team|. [online] Available at: <https://www.cirt.gov.bd/>.

Team, C., 2021. *Bangladesh Cyber Threat Landscape Report 2020*. [online] BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team. Available at: <<https://www.cirt.gov.bd/bangladesh-cyber-threat-landscape-report-2020/>>.

Trmcic, A., Demmings, E., Kniel, K., Wiedmann, M. and Alcaine, S.D. (2021). Food Safety and Employee Health Implications of COVID-19. *Journal of Food Protection*. doi:10.4315/jfp-21-201.

Tuffield, D. (1975). *Organization behavior Ind. Commer. Train.*, 7, (4), pp. 164–166.

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, p.102387. doi: 10.1016/j.cose.2021.102387.

Uddin, M. (n.d.). THE NATIONAL CYBERSECURITY STRATEGY OF BANGLADESH: A CRITICAL ANALYSIS. [online] Available at: <https://www.biliabd.org/wp-content/uploads/2021/09/Md.-Riaz-Uddin.pdf>.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7(1), pp.50–58. doi:10.1108/09685229910255223.

Von Solms R. (2004). From policies to culture. *Computer & Security* 23, pp.275-279.

Von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, 25(3), pp.165–168. doi: 10.1016/j.cose.2006.03.004.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, [online] 38, pp.97–102. doi: 10.1016/j.cose.2013.04.004.

Wahl, A. and Bull, G.Q. (2014). Mapping Research Topics and Theories in Private Regulation for Sustainability in Global Value Chains. *Journal of Business Ethics*, [online] 124(4), pp.585–608. Available at: <https://www.jstor.org/stable/24033179>.

Wahyuni, D. (2012). *The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies*. [online] Ssrn.com. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2103082](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103082).

Westby, R. J., 2007. *Governing for Enterprise Security (GES) Implementation Guide*. 1st ed. [eBook] Pittsburgh, United States: Carnegie Mellon University, p.116. Available at: <<http://www.sei.cmu.edu>>.

Whitman, M. and Mattord, H. (2014). *Management of Information Security*, 4th Edition. 2014 Faculty Bookshelf. [online] Available at: <https://digitalcommons.kennesaw.edu/facbooks2014/42/>

Yaokumah, W. (2013). Evaluating the Effectiveness of Information Security Governance Practices in Developing Nations: A Case of Ghana. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, [online] 4(1), pp.27–43. Available at: <https://ideas.repec.org/a/igg/jitbag/v4y2013i1p27-43.html>.

Zimmermann, V. and Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, pp.169–187. doi: 10.1016/j.ijhcs.2019.05.005.



With a view to get the answers of the Research Questions, it have had formulated the following

Interview Questionnaire

- a. Organizational IT setup-
  - a.1 Which organization is it and how many employees are there in the IT cell?
  - a.2 When did you start Information Securitization in your office?
  - a.3 Does your organization go on with any approved security policy /standard?
  - a.4 For any Information incident, to whom you are to report to?
  
- b. Information Security attacks and threats related-
  - b.1 Have you suffered a breach of Information in last two years?
  - b.2 Which types of security threats you generally encounter in your systems?
  - b.3 How did the threats affect your organization?
  - b.4 What do you think to be your highest security risks?
  - b.5 How secure do you think your organization's Information systems?
  
- c. Preventive technologies/ actions-
  - c.1 What measures do you often activate to reduce damage from attacks at your institution's Information architecture?
  - c.2 Which security plans have your organization adopted?
  - c.3 How do you anticipate about new forms of risks, vulnerability and threats?
  - c.4 How do you detect attack?
  - c.5 In order to raise Information security awareness, does your office provide employee training?
  
- d. Monitoring and reaction to the identified security threats-
  - d.1 Does your organization have the ability to execute deep-packet inspection?
  - d.2 Has penetration testing ever been accomplished in your office?
  - d.3 How you ensure appropriate level of security over third parties?
  - d.4 What do you think about further improving your organization's Information security level?
  - d.5 How difficult is it to persuade the administration to spent more money for security solutions?

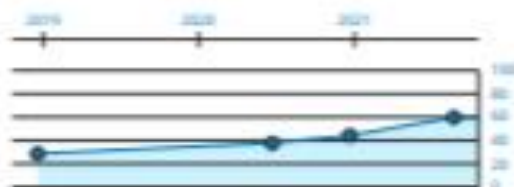


## 41. Bangladesh 59.74

Population: 161.8 million  
 Area (km<sup>2</sup>): 147.6 thousand  
 GDP per capita (\$): 4.5 thousand

41<sup>st</sup> National Cyber Security Index: 62 %  
 53<sup>rd</sup> Global Cybersecurity Index: 81 %  
 147<sup>th</sup> ICT Development Index: 25 %  
 105<sup>th</sup> Networked Readiness Index: 36 %

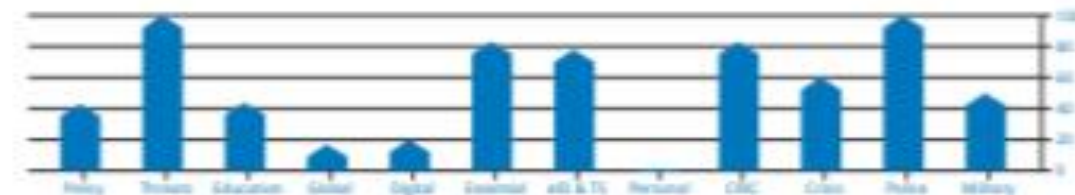
### NCSI DEVELOPMENT TIMELINE



### RANKING TIMELINE



### NCSI FULFILMENT PERCENTAGE



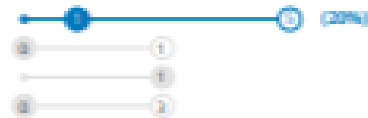
### GENERAL CYBER-SECURITY INDICATORS



## BASILINE CYBER SECURITY INDICATORS

### 5. Protection of digital services

- 5.1. Cyber security responsibility for digital service providers
- 5.2. Cyber security standard for the public sector
- 5.3. Competent supervisory authority



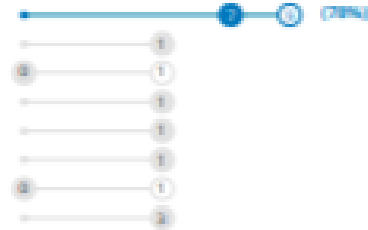
### 6. Protection of essential services

- 6.1. Operators of essential services are identified
- 6.2. Cyber security requirements for operation of essential services
- 6.3. Competent supervisory authority
- 6.4. Regular monitoring of security measures



### 7. E-identification and trust services

- 7.1. Unique persistent identifier
- 7.2. Requirements for cyptosystems
- 7.3. Electronic identification
- 7.4. Electronic signature
- 7.5. Timestamping
- 7.6. Electronic registered delivery service
- 7.7. Competent supervisory authority



### 8. Protection of personal data

- 8.1. Personal data protection legislation
- 8.2. Personal data protection authority



## INCIDENT AND CRISIS MANAGEMENT INDICATORS

### 9. Cyber incidents response

- 9.1. Cyber incidents response unit
- 9.2. Reporting responsibility
- 9.3. Single point of contact for international coordination



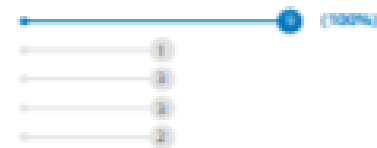
### 10. Cyber crisis management

- 10.1. Cyber crisis management plan
- 10.2. National-level cyber crisis management exercise
- 10.3. Participation in international cyber crisis exercises
- 10.4. Operational support of volunteers in cyber crises



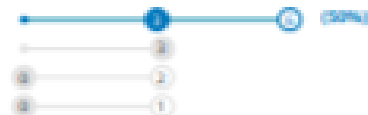
### 11. Fight against cybercrime

- 11.1. Cybercrimes are criminalised
- 11.2. Cybercrime unit
- 11.3. Digital forensics unit
- 11.4. 24/7 contact point for international cybercrime



### 12. Military cyber operations

- 12.1. Cyber operations unit
- 12.2. Cyber operations exercise
- 12.3. Participation in international cyber exercises



EGA is held and developed by  
e-Governance Academy Foundation  
Company code: 60871660

Belmontstr. 8  
10111 Berlin  
Germany

T +49 30 663 1100  
E [info@ega.eu](mailto:info@ega.eu)  
W [www.ega.eu](http://www.ega.eu)