Information Security Policy Guideline, Bangladesh

(Draft)

অপনার গুরুত্বপূর্ণ মতামত নিম্নলিখিত ই-মেইলে প্রেরণ করা যাবে।

ict.ministry@yahoo.com
jsict@moict.gov.bd
ict1@moict.gov.bd

Information Security Policy Guideline, Bangladesh (Draft)

Bangladesh Computer Council

Ministry of Information and Communication Technology

Government of the People's Republic of Bangladesh

Document Information

Document Title	**Information Security Policy Guideline, Bangladesh**
Document Type	**Public**
Version	**1.12.12.00**
Commencement Date	
Last Update	**January 2013**
Pages	**32**
Status	**Draft**

Table of Contents

1. Preamble

Government of the Peoples Republic of Bangladesh intends to materialize the Vision 2021: Digital Bangladesh. To achieve this vision, all government agencies will be brought under the e-governance framework. Different government Ministries/Divisions, Departments/agencies and their subordinate bodies have started implementing e-Governance. The intention is to improve & ease the government work process and to increase the productivity of the government. While doing this, it is required to digitize the government information, to process and store those digitized information in a manner so that the information doesn't get lost or the information is not manipulated. It is very important to consider information security for a government while implementing e-Governance. This document is a guideline to help government agencies to formulate their own **Information Security Policy** to protect their information in the cyber space.

In recent past, Bangladesh especially the government sector has faced number of cyber attack incident (e.g. web defacement, information damage, information theft, Distributed Denial of Service, etc.). In most of the case the reasons are:

- lack of information protection procedure,
- weak and unmanaged security controls,
- under skilled personnel and lack of expertise,

Currently, there are no preventive, reactive, detective and administrative security measures to protect digitized government resources. To protect digitized government resources from unauthorized access this is fundamental requirement to have proper security policy and implementation mechanism in place.

This document is a baseline document prepared by Bangladesh Computer Council for any agency who wants to formulate their information security strategy with an intention to protect their digitized information in the cyber space.

This is a live document which will be made up to date as necessary from time to time since information technology is something that's keep changing with time.

2. Introduction

Information is the most valuable asset for an agency. Information has different dimension in terms of accessibility. Some information is public where as some are confidential. Depending on the degree of confidentiality, information has several level of accessibility as well. Such as there are information which are open for public access without any authentication of the information seeker, some are accessible with single factor authentication, some require multi factor authentication whereas some are private within the organization, some are highly confidential that only a group of people in an organization has access. So it is very important for an agency to have clear understanding about their information and the accessibility. Before preparing an Information Security Policy it is recommended for an agency to classify their information through proper assessment.

Internet is an open platform for all to access information. Internet technology and other technologies like handheld devices, mobile devices, tablet PCs, wireless technologies are making information easily accessible and affordable. There may be some situation when information can be used as weapon to make chaos in a country. So it is the duty of an agency to take care of its own information in the internet. Apart from information in internet, the agency should also be aware of the information that may have different state such as information that's moving in the intranet or LAN or in the cloud or simply stored in an internal database or in a PC.

This guideline covers:

- Brief illustration of different terminology that's important to know while preparing Information Security Policy,
- Objective of this guideline,
- Scope of this guideline,
- Information classification and different state of information,
- Roles and responsibility of the information owner and information custodian,
- Information security strategy,
- Identification of probable risks, threats and vulnerabilities,
- Assessment of risks, threats and vulnerabilities,
- Procedure to set security controls to protect information,
- Legal issues of information security,
- Standards to follow to establish Information Security Management System (ISMS),
- Importance of auditing for information security,
- Monitoring and improving,
- Certification as an agency,
- Procedures for incident handling and disaster recovery,
- Backup & restore mechanism,

- Business continuity plan,
- Sample Information security policy

The above mentioned issues will be discussed throughout this document.

3. Guideline Governance and Enforcement

Ministry of ICT on behalf of the Government of Bangladesh will have the ownership of this guideline. Ministry of ICT will monitor the implementation of this guideline. Bangladesh Computer Council, Office of the CCA and Bangladesh Telecommunication Regulatory Commission (BTRC) will jointly coordinate the implementation of this guideline.

All the agencies of Bangladesh Government are requested to develop their own Information Security Policy and implement accordingly within six (6) months of its commencement.

Any query regarding this document can be forwarded either to Ministry of ICT or to BCC. If any agency require assistance for preparing their **Information Security Policy** may request support from BCC.

4. Definition

Agency: Agency includes ministry/division, departments and sub-ordinate bodies of the Government of Bangladesh.

Asset: Anything of value to an agency.

Attack: Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Authentication: Provision of assurance that a claimed characteristic of an entity is correct.

Authenticity: Property that an entity is what it claims to be.

Availability: Information Systems available to users at any given or specified period of time and being accessible and usable upon demand by an authorized entity.

Business continuity: Processes and/or Procedures for ensuring continued business operations.

Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, systems or processes.

Certification: Certification is something provided by any standard bodies or by some form of external review to an agency after evaluating their information system infrastructure and information security management system.

Classified Information: It refers to the categories of information classified in accordance with the Security Regulations.

Control: It means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure.

Control objective: Statement describing what is to be achieved as a result of implementing controls.

Corrective action: Action to eliminate the cause of a detected nonconformity or other undesirable situation.

Eavesdropping: Eavesdropping, an unauthorized access to information, is a kind of network attack by capturing packets while communication/transmission of information.

Exploit: A technique or code that uses a vulnerability to provide system access to the attacker.

Guideline: A description that clarifies what should be done and how, to achieve the objectives set out in policies information processing facilities any information processing system, service or infrastructure, or the physical locations housing them

Information: Digitally processed data or digitized information of an agency or an individual.

Information asset: Information or data that has value to the agency or individual.

Information System: An electronic information system that processes data electronically through the use of information technology - including but is not limited to: computer systems, servers, workstations, terminals, storage media, communication devices, network resources and Internet.

Integrity: When authorized persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

IS Policy: A documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction.

Information security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

Information security event: An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information security incident: An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

PKI: PKI is a framework that consists of hardware, software, policies, and procedures for managing keys and certificates.

Policy: Overall intention and direction as formally expressed by management

Risk: Combination of the probability of an event and its consequence

Risk analysis: Systematic use of information to identify sources and to estimate the risk

Risk assessment: Overall process of risk analysis and risk evaluation

Risk evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

Risk management: Coordinated activities to direct and control an organization with regard to risk

Risk treatment: Process of selection and implementation of measures to control or minimize risk

Social engineering: Obtaining information from individuals by trickery.

Spoofing: A form of masquerading where a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.

Third party: That person or body that is recognized as being independent of the parties involved, as concerns the issue in question

Threat: A potential cause of an unwanted incident, which may result in harm to a system or organization

Vulnerability: A weakness of an asset or group of assets that can be exploited by a threat

5. Objective

Information is an important asset for an agency as well as for a state. Protecting information is vital to establish and maintain trust among government, citizen and business entities. Information security is the process, involved with the people and technology of an agency, by which that agency protects and secures its information. Information Security Policy defines set of rules and control mechanism to protect information against attacks or threats or misuses or damage or unauthorized access.

The objective of this guideline is

- to help agencies of the Government of Bangladesh to understand the nutshell of Information Security,
- to define the methodology to prepare Information Security policy,
- to give them proper guidance to implement Information Security Policy,

Since one of the major objectives is to assist users of this guideline to prepare Information Security Policy, they must know that the policy document is an internal document within the agency/organization and the stakeholder for such policy is mostly internal within the agency/organization.

6. Scope

All government, semi-government, autonomous agency or public limited company in Bangladesh who wants to prepare their Information Security Policy document, can use this guideline. This is a baseline for them to prepare their policy to protect their information. Any private organization inside Bangladesh can also adopt this guideline.

7. Information Asset

This section will assist the key members of an agency to redefine their idea on agencies information/data. It'll help them to understand how to define states and classify their information asset, set ownership and custody for different information asset and safeguarding the information asset according to the defined roles and responsibilities.

7.1. Definition of Information

Information is an asset that, like other important business assets, is essential to an organization's business and consequently be appropriately safeguarded.

Broadly defined Information is the basis on which the agency conducts their business. Reliable information supports business capabilities, notably by enabling good decision making. The Government holds information that is operationally, administratively, politically, commercially or personally significant. The government has a fundamental 'duty of care' and legal obligations to protect this information from unauthorized or accidental modification, loss/damages or release. There are moral and ethical considerations in the appropriate handling of information as well.

Information can be in any form. It includes:

- documents and papers;
- electronic data;
- the systems (software, hardware and networks) on which the information is stored, processed or communicated;
- intellectual information (knowledge or perceptions) acquired by individuals;
- physical items from which information regarding design, components or use could be derived; and
- Images, audio or video clips.

7.2. Definition of Information Asset

Asset is anything that has a value to the organization, agency or nation. Information is a key asset for an organization. Asset must keep in protection for ensuring trust among stakeholders who use and own the asset. Asset is very much related to security risks assessment. The first step in assessing security risks is to take stock of your enterprise's information assets (e.g. application programs, stored data, reports, product designs and specifications, proposals, business plans, financial records, databases, and other files and documents residing on your organization's computer systems)

The objective is to organize the assets, conceptually, into appropriate categories, to help understand them and their boundaries. It is necessary to determine the appropriate owners of

the various assets and convince them to take responsibility for evaluating their importance and value.

Asset must be classified for assigning access to that asset. Once the information resources have been identified and developed appropriate ways of classifying and understanding their perimeters, the next step is to define who needs access to what information. There are many types of assets including but not limited to:

- databases and data files, contracts and agreements, system documentation including process, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- application software, system software, development tools, and utilities;
- computer equipment, communications equipment, removable media, and other equipment;
- computing and communications services;
- people, and their qualifications, skills, and experience;
- intangibles, such as reputation and image of the organization

Information is created, processed, stored, archived, and deleted while executing business activities. Examples are database records, mails, source code, paper documents, designs, emails, databases, Process Data, images etc.

An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. The most important and valuable information assets are those underpinning an agency's core or most critical duties, capabilities or goals. The value of information assets is expressed in terms of the potential business consequences for events resulting in loss of confidentiality, integrity and or availability to them. Potential consequences include direct and indirect financial losses (immediate or subsequent), loss of revenue, failure to meet service obligations or reputational loss. Indirect consequences of a security failure also have to be considered.

Information asset valuation can be done in terms of,

- Confidentiality of Information Asset;
- Integrity of Information Asset;
- Authenticity of Information Asset;
- Non-repudiation; and
- Availability of Information Asset.

7.3. Different State of Information

As mentioned earlier information has different form of presence. It has different state as well. It is very important for an agency to consider those states while developing their policy for Information Security. Common states of information are:

- Information that's been archived (Historical information)
- Agencies private information or personnel information stored in database or tape drive or in any media
- Regular business information processed in applications
- Static and dynamic information in the website of the agency
- Communication/correspondence, perception and knowledge
- Information that's processed in the Intranet of the agency/government
- Information that's processed in the internet of the agency/government
- Information that's processed in the extranet

Different state of information needs different security mechanism. This shall be done considering the importance of the information as well by classifying information as required. It's much easier and convenient to impose security controls for same group of information depending on their nature of importance. Every agency shall find out the states of its information and define in the security policy along with the classified information.

7.4. Information Classification

Information of different types needs to be secured in different ways. Therefore a classification system is needed, whereby information is classified, a policy is laid down on how to handle information according to its class and security mechanisms are enforced on systems for handling information accordingly. Information classification ensures information receives an appropriate level of protection. Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

Information can be classified in terms of its value, legal requirements, sensitivity, and criticality to the country or to the agency. Classification systems vary from country to country, agency to agency. In most countries, the common classification has five levels as mentioned below:

1. Top Secret
2. Secret
3. Confidential
4. Restricted
5. Public or Unclassified

While classifying information asset, it is recommended to check compliance with government laws and regulations. The agency may decide to have own way of classification with more or less number of levels. But it is the prior most important job of an agency to analyze their information and define the states and classification. Accordingly, the agency shall impose security controls.

7.5. Information Owner

The **Information owner** is a functional owner responsible for ensuring information classification with different state, proper controls are in place to address confidentiality, integrity, authenticity and availability of information. Information owner has authority and responsibility for controlling production, development, maintenance; using security controls over the asset; placing appropriate level of protection; reviewing the information classification, security controls, access restrictions periodically for making cost-benefit decisions essential to ensure accomplishment of organizational mission objectives.

7.6. Information Custodian

The **Information custodian** is a person designated by the owner to be responsible for protecting information by maintaining safeguards and controls established by the owner; taking prior approval before sharing information. A custodian is also responsible to perform regular backup and data validity testing activities, data restoration from backups periodically, implement access control as defined by information owner. Custodian should be assigned for each information asset. The custodian remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

7.7. Roles and responsibilities

Agencies are responsible and accountable for appropriately safeguarding the information assets in their custody. Agencies are best able to gauge the significance and worth of their information assets, the risks to them and the appropriate measures to safeguard them. The approach is to achieve and maintain appropriate protection of organizational assets. To accomplish this goal, all assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The information/asset owner has the responsibility of to define the classification of information/asset, periodically review it, and ensure it is kept up to date and at the appropriate level of security controls. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the information assets. One of the very important obligations for any agency is not to outsource the responsibility of their information, i.e. responsibility for the security of information assets should kept always within the agency owning that.

7.8. Archiving of Information Asset

Continuous accumulation of information will be voluminous and may go beyond the manageable limit resulting difficulties in handling information for its optimum utilization. Therefore obsolete, duplicate, redundant and unnecessary information may be destroyed or archived. While destroying any information an agency must get proper approval for destroying from information owner and custodian, and they must maintain a log mentioning reason for destroy. In case of archival, similar to archival of paper and files, an agency must consider archival of electronic information asset. Depending on the importance of information asset agency may define retention period of information asset. An agency must follow Section 9 of ICT Act 2006 and other relevant law before defining the retention period of electronic information.

7.9. To Dos according to this Section

The tasks defined in throughout section 6, are the prior tasks of an agency that should be structured properly in their Information Security Policy. As a whole, this is called information gathering and information asset management. Steps towards accomplishing this include:

1. **Information classification and state**
   Information should be analyzed and classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. After classification, the states of those classified information must also be defined.
2. **Inventory of Information assets**
   All information assets should be clearly identified and an inventory of all important assets drawn up and maintained. An agency should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.
3. **Information labeling and handling**
   An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. Procedures for information labeling need to cover information assets in physical and electronic formats.
4. **Ownership of Information assets**
   All information and assets associated with information processing facilities should be owned by a designated part of the organization. The asset owner should be responsible for:
   - ensuring that information and assets associated with information processing facilities are appropriately classified;

- defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

5. **Acceptable use of Information assets**
   Rules for the acceptable use of information assets associated with information processing facilities should be identified, documented, and implemented. All employees, contractors and third party users should follow rules.
6. **Responsibilities**
   Owners, custodian and others should be identified and assigned with the responsibility of information asset management within an agency. Their responsibilities shall be clearly defined and reviewed periodically for seamless protection of information asset. Archival of information and retention period of information asset must also be considered while defining the responsibilities.

8. Strategy for Information Security

Agency before preparing its Information Security Policy should set a plan for integrating process, people, technology, procedures to safeguard its information from threats. The strategy should be reviewed periodically to mitigate newer threats and vulnerabilities in the area of information security. This section will assist the agency to understand the best practices of Information Security Strategy in the globe and will help them prepare their own strategy or adopt available best practices.

8.1. Preparing Strategy

Information security strategy is not necessarily being something that is the best practice in the world. It's important to understand the best practices to prepare own strategy but it is not always rational to adopt the best practices only. Accepting best practices only may leave the policy strategy unworkable and unrealistic. So, it's always recommended to prepare strategy blending the real world and best practices as required by an agency. Information security strategy has the following stages:

- Objective
- Understanding
- Plan (Policy, Procedures, Standards, Guidelines, Controls, etc.)
- Implementation
- Check Compliance
- Monitoring & Review

8.1.1 Stage 1: Objective

There must be an objective for an organization/agency to adopt information security strategy. For most organization/agency the objective is to safeguard their information from threats in the cyber space. Threats of information theft or loss may disrupt the goal

and productivity of an agency. So the agencies should set their objective to protect their information from threats.

8.1.2 Stage 2: Understanding

Before start developing security policy for the agency, it is required to have a thorough understanding of the agency. It is also required to consider the goals and direction of the agency. The policy that is going to be developed must also conform to existing policies, rules, regulations and laws that the agency is subject to. In this stage, before developing the policy, it is also required to gather information to identify the information assets; to identify the risks, vulnerabilities & threats; to identify potential safeguards & controls with associated cost and percentage of risk reduction; and to re-define roles and responsibilities.

8.1.3 Stage 3: Plan

With the gathered information of stage two (2) and considering the objective the agency shall prepare its security policy in this stage. This stage may include procedures, standards, guidelines etc along with the policy. While preparing the security policy it is recommended to the agency to take assistance and check compliancy with **ISO/IEC 27002: Code of Practice for Information Security Management**. While developing the policy, the agency should consider the location of their information asset, whether they are putting it inside their domain or outside. The government agency must keep their information asset inside the country. And it is recommended to the government agencies to keep their information asset in the National Data Center hosted in BCC.

Before putting the policy in action, it is recommended to organize consultation among the implementer and stakeholders of the policy. Such consultation will help produce effective security policy.

8.1.4 Stage 4: Implementation

After preparing the policy and other supporting procedures or guidelines, the agency shall educate its personnel and distribute these to all its implementers (management, BOD, employees etc.) and take their agreement that they read & understood the policy and agreed to comply with it.

The key to acceptance and compliance with security policies is education. Educating employees on the need for security and keeping them involved in the policy development process is important to keep them from finding ways to avoid policies and rendering them ineffective. Seminars and awareness campaigns help to educate the importance of security, especially on password selection, screen locking, document labeling, and physical security. Helpdesk in the preliminary stage for successful implementation may also be introduced.

8.1.5 Stage 5: Check Compliance

It is always recommended that the agency must develop a method to measure compliance with the policy and check compliance in a periodical basis. This compliance method may include the formation of auditing team to ensure that the policy is enforced. The auditors who are responsible for monitoring compliance with the security policy should be independent of the persons implementing the policy. The policies must be enforced in a strictly manner and noncompliance of the policy is punishable.

8.1.6 Stage 6: Monitoring & Review

It is important to have monitoring and review mechanism for future improvement since new threats are being discovered as time passes by. Monitoring & review includes changes in the organization resulting in new threats. Security controls have to be modified as necessary to mitigate any new threat introduced. Training is vital issue that might need to arrange for performance improvement. As time goes by, it is crucial to maintain the relevancy of the security policies. New policies may be added when necessary.

8.2. To Dos according to this section

In this section, the strategy for information security is defined. It is the whole life cycle for an agency to work out to develop an Information Security Policy so is to successfully protect their information assets.

The stages defined in this section must be followed by agencies to safeguard their valuable information from threats. To dos in previous section (section 6.8) is part of the stages in the strategy defined earlier. The audiences of this policy guideline are requested to not create any confusion on what to do first. The audiences, who want to prepare information security policy for their agencies, should start with the stages defined in section 7.1. All other sections are to assist completing these six (6) stages.

9. Risk, Threats and Vulnerabilities

While formulating a security policy every organization or agency should be aware of possible risks that can affect the safety and security of their information asset. The organization or agency should also have clear understanding about threats and vulnerabilities that could damage its information assets. For appropriate safeguard of information assets know-how on risks, threats and vulnerability is vital. This section will assist an agency to understand and identify and analyze threats, risks and vulnerabilities.

9.1. Understanding Risk, Threat and Vulnerability

Risk

The potential (merely “chance”) for loss, damage or destruction of an information asset as a result of a threat exploiting a vulnerability. Reducing the risk of an organization requires risk

identification and risk management process to be done periodically. An agency should know major risks that may cause potential loss of their information asset. Reasons for major risks/weaknesses are:

- little support for security measures,
- information is not classified,
- inadequate information security policy operates,
- lack of security awareness are there,
- weak access control mechanisms exists,
- no official policy and no monitoring/intrusion detection or incident response team are in place,
- Operating procedures are not documented,
- Employees are not identified adequately, visitors may roam unchecked,
- The building is in an earthquake zone, where minor quakes are expected,
- The building is in an flooded zone or can be affected by flood because of lack of proper water disposal system,
- Lack of fire prevention system, etc.

Threat

A threat is a potential cause of an unwanted incident, which may result in harm to a system or organizations' information assets. Threat is anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy of an asset.

Threats can be occur by natural disaster, intentional or accidental acts originating inside or outside the agency. Most threats exploit vulnerabilities in information assets or their supporting infrastructure (hardware or software). Typical information security threats that could cause unwanted event include:

- unauthorized access,
- disclosure of information,
- legal threats,
- sabotage,
- inadequate security awareness,
- poor security policy,
- fraudulent,
- workload,
- denial of service,
- spoofing,
- advanced persistent threat (APT),
- applications with bugs,
- eavesdropping etc.

Vulnerabilities

Vulnerabilities are flaws or weaknesses associated with an agency's assets or capabilities. Vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Therefore, a vulnerability that cannot be exploited by a threat or an asset with no known or suspected vulnerabilities cannot be a security risk. Typically vulnerability results from:

- flawed procedures,
- under-skilled staff,
- incorrectly configured or defective technology.

For a vulnerability to be exploitable it must be known to or discoverable by a threat. This makes it important to follow the 'need to know' principle with respect to security related information, and apply it to both people and technology. It also makes it important for an agency to react appropriately when learning of vulnerabilities or vulnerabilities that affect it. However, the most pervasive vulnerability is probably the susceptibility of staff to 'social engineering', which makes security awareness for all staff an important safeguard. Vulnerabilities are classified according to the related assets:

- Organizational
- Personnel
- Environmental
- Hardware, software and network
- Spatial

9.2. Identification of Risk, Threats, and Vulnerabilities

Information Security Policy is needed for an agency to protect their information asset from risks (that may cause damage or lose of information asset) caused by threats exploiting certain vulnerabilities. It is always seen that most agencies always mix up the definition of risk, threat and vulnerability. Risk, threat and vulnerability are not terminologies for same meaning. For clear understanding of these three terms, following is a good simple relational definition between information asset, risk, threat and vulnerability:

Information Asset	Threat	Vulnerability	Risk
Information asset is something what agency tries to protect.	Threat is something against what an agency tries to protect their information asset.	Vulnerability is the weakness or gap in the protection efforts made by an agency.	Risk is destruction (or chance of destruction) of an information asset as a result of threat exploiting vulnerability.

It is important for every agency to identify risk, threat and vulnerabilities to their information system and applying security controls accordingly. Classification of information and state of information will make the job easier for an agency to do the risk assessment and to apply security controls. An agency must define scaling factor for all its identified risks in terms of severity of the risk. This scaling factor must be defined in numerical scale and from 0 to 10 where 0 is for low and 10 is for high.

9.3. Risk Management

The objective of the risk management process is to identify threats and vulnerabilities and to provide recommendations to ensure protection of information asset. The risk management process can be done with internal or external resources. Area that an agency must consider before risk management process, are:

- Network and software design and development,
- Change management,
- Physical security, Access control,
- External vulnerability, Internal vulnerability,
- Storage and backup strategies, restoration procedure and testing
- Contingency planning/testing (disaster recovery/business continuity),
- Information transmission,
- Disposal of information assets,
- Personnel skill,
- incident management history,
- Systems audit practices, etc.

An agency must define its risk management process while producing the IS Policy. A model has been developed by a project called CORAS of EU based on AS/NZS 4360:2004 and ISO/IEC 31000:2009 which is a very good and acceptable model for risk management. This model can also be adopted by any agency in Bangladesh or they can develop their own model.

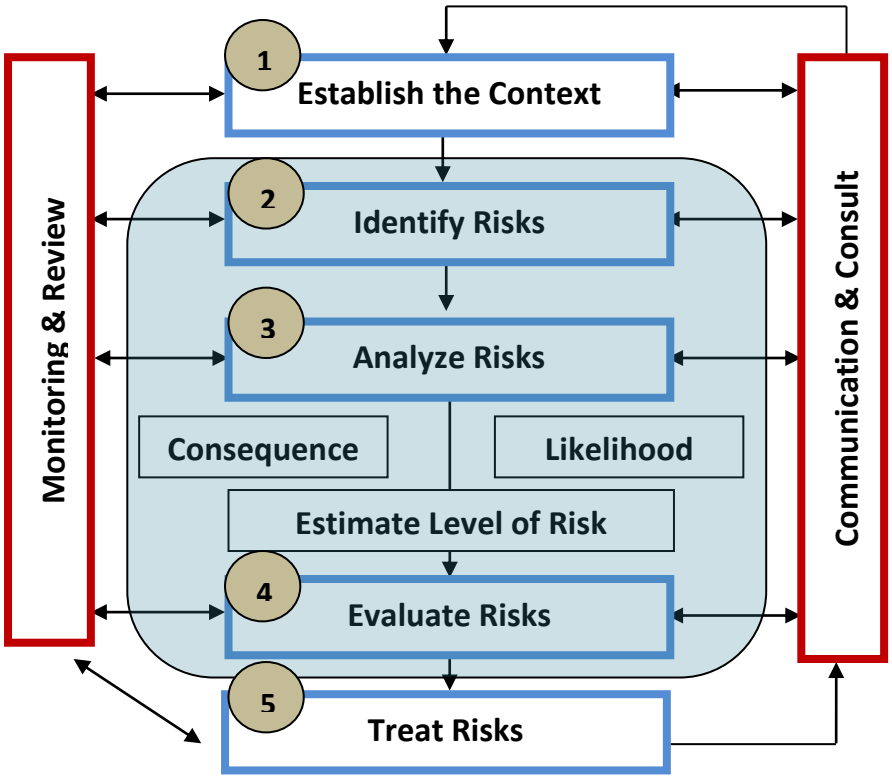

Figure 1: Risk Management Process

There are 5(five) steps in Risk Management process shown as circle in the figure. The vertical boxes: Monitoring & Review and Communicate & Consult is necessary in every steps of risk management process for effectiveness and improvement. The stages in risk management process are:

Establish the context

The purpose of the context establishment is to characterize the target of the analysis and its environment. There could be external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis to be defined.

Identify Risk

In this stage, the agency must identify where, when, why and how incident can happen, that is identification of threats; what can trigger an incident, that is identification of vulnerabilities. While doing this, it is recommended to do considering the classification of information assets.

Analyze Risk

This is the stage where an agency will do the risk estimation. Here an agency will identify and evaluate existing controls. Then the agency will determine the consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.

Evaluate Risk

This is a very important stage to make decision how to treat a risk. In this stage, on the basis of the result of analyzing risks, an agency will map the resulting risks with their associated risk values to decide how to treat risks. There might come some risks where no treatment is required. Here the agency will make a priority for treating risk.

Treat Risk

As per the result came from previous stage, the agency may prepare effective plans and procedure to mitigate the risks. It is always recommended to prepare plans with maximum effectiveness and minimum cost. Treating risk may include risk avoidance, risk transfer, retain risk, changing likelihood and consequences of the risk.

9.4. Risk Management Template

An agency must prepare a template for its risk management process. And this risk analysis process must be a periodical process over the lifecycle of an agency. Risk assessment template is a simple form with fields that an agency will periodically fill up after completing the risk analysis. In this guideline, a sample template is given below:

Information Asset		Threat Analysis		Vulnerability Analysis		Risk Analysis		Action Plans to mitigate	Remarks
Details	Class & State	Name	Details	Name	Details	Details	Level		

9.5. To Dos according to this section

This section describes the function related with several stages of Information Security strategy defined in section 7.1, especially in Stage 2: Understanding, Stage 4: Implementation and Stage 6: Monitoring & Review. Risk management is more an action than just a policy. An agency while preparing its Information Security Policy document may include the methodology/model of risk assessment along with just definition and reasons for having this. The following things are recommended to include in the methodology/model for comprehensive risk management:

- Frequency of Risk Assessment,
- Information Gathering,
- Threat & Vulnerability Analysis,
- Risk Identification,
- Risk Analysis & Evaluation,
- Risk Treatment,
- Monitoring & Review,
- Risk assessment Template.

Risk management is a very important part for protecting information assets. In this section, issues related to risk management has been described briefly. For more detail, an agency may go through ISO/IEC 27005, ISO/IEC 31000, AS/NZS 4360:2004 and “A Platform for Risk Analysis of Security Critical Systems” by CORAS of EU.

10. Security Controls to protect information

Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks. To help review or design security controls, they can be classified by several criteria. For example according to the time:

- Before the event, preventive controls;
- During the event, detective controls;
- After the event, corrective controls.

Security controls can also be categorized according to their nature, for example:

- Physical controls
- Procedural controls
- Technical controls
- Legal and regulatory or compliance controls

There are a number of best practices in the world where number of information security controls/governance are defined, those are:

- ISO/IEC 27001, ISO/IEC27002
- CoBIT 4.1 or above
- ITIL V3 or above

The security controls defined in the above best practices are generic and an agency must tailor those standards or best practices as per their need in a cost effective way. It is optimized to consider the classification of information asset while adopting the security controls. There's no need to adopt very rigid security controls for information asset that is not secret. Example of some security controls (taken from ISO/IEC 27002):

- Personnel Security,
- Equipment Control,
- Access controls,
- Physical and Environmental Protection,
- Operational Procedure and responsibilities,
- Third party service delivery management,
- System planning and acceptance,
- Application Security,
- Protection against malicious code,
- Information back-up,
- Network security management,
- Removable Media handling,
- Information exchange/transmission,
- Information disposal,
- Information system security,
- Cryptographic controls,
- Correct processing,
- System files security,
- Monitoring, etc.

It is recommended to go through ISO/IEC 27002 to know more about these controls. And agency must decide to adopt controls wherever and whatever they need to protect their information.

National PKI which is recognized by the ICT Act 2006, is already available in the country and it is under regulation of Office of the CCA, Ministry of ICT. An agency must use digital signature certificate and PKI enabled applications to ensure their cryptographic controls. Digital Signature certificates ensures 4 goals of Information Security, those are:

- Authenticity (authenticity of information and parties involved in information exchange)
- Confidentiality (ensures confidentiality of information using encryption technology)

- Integrity (assures information user about the alteration of information)
- Non-repudiation (information originator or signer can not challenge legally that (s)he or they did not sign or originate the information)

11. Legal and Compliance Issues

While preparing the policy the agency must be aware of legal and compliance issues that may be affected if the policy put in place. This is important to consider both internal and external legal and compliance issues to avoid breaches of any law or regulatory obligations and to avoid contradictions with other policy. List of some legal and compliance document that an agency must consider while developing their policy:

- ICT Act 2006 (amended in 2009)
- ICT Policy 2009
- Right to Information Act
- Intellectual Property Rights
- Copyright, Patent, Trademark related laws
- PKI related rules/guidelines for cryptographic controls
- Laws on document & records retention
- Cyber Security related laws/guideline/policy (if any)
- UN conventions/Laws related to internet or cyber security

An agency within the government must formulate such a policy which will comply with national laws, policies and guidelines. In the IS Policy document, an agency must mention the name of the legal documents and other policies/guidelines/standards the policy complies with.

An agency must consider Service Level Agreement (SLA) in place before taking any services from the vendor or from any other government agency related to ICT (Hardware, Software, Network or any other information system)

12. Standards and Guideline

The Information Security Policy of an agency does not define any step by step procedures to implement the policy and does not explain any standard the agency is following for the successful implementation of the policy. Standards and guidelines come when the policy is in place. But there must be some guidance in the policy document so that the agency must set the standards and guideline they are going to follow in every stage of protecting their information asset. There may be number of guidelines and standards under a policy document depending on the requirement.

13. Information System Audit and Certification

In the context of Bangladesh, agencies those handle critical information system infrastructure, must go through IS audit periodically. The auditor in this case can be internal or external or both. IS audit is very significant to minimize disruptions in operational procedures and to improve performance. IS Audit is part of Stage 6: Monitoring & Review of Information Security strategy.

Certification is something provided by some form of external review by a third party to an agency after evaluating their information system infrastructure and information security management system. The evaluation criteria are always maintained by the standard bodies. Certification gives assurance to internal and external stakeholders about an agency. If an agency wants to get certified in compliance with ISO/IEC 27001, they are suggested to check the evaluation criteria from ISO/IEC 27007 beforehand. Bangladesh Computer Council (BCC) as per their rules of business may start certification activities for the agencies implementing ISMS. Quality certification enables organized working environment and let the agencies improving their performance.

14. Incident Management

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. In the area of Information Security, it is very crucial to consider incident management plan before an incident occur. No one can exactly know when and what incident is coming to impede the business process beforehand. Information security incidents may occur at any time. It is very important to establish robust and effective processes to deal with incident.

Incident can be natural or human driven. For both case, effective incident management depends how well the management is responding an incident. In case of natural incident, for example, in case of flood or fire or earthquake or any type of natural calamity it is recommended to start with recovery of the information system for business continuity.

Incident can be driven by human intervention in a form of attack, in case of human driven occurrences, Information security incident shall be reported through appropriate management channels as quickly as possible. Internal or external expert or Information Security Incident Response Team must be involved after an incident to investigate and report properly. It is also important to know by all the internal employees to leave the evidence unchanged after an incident occurred. After successful investigation of an incident, it should be recorded for improvement in the risk management system. And the assessment report on

incident must be forwarded to the management for taking necessary actions wherever necessary.

In the Information Security Policy document there must be some direction of incident management. It is suggested for every agency to go through ISO/IEC TR 18044:2004 for better understanding on Incident Management.

15. Business Continuity Plan

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption, a business continuity management process should be implemented. It is important to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

Information security should be an integral part of the overall business continuity process, and other management processes within the organization. Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available. Steps in Business continuity plan (as per ISO/IEC 27002):

- Including information security in the business continuity management process;
- Business continuity and risk assessment;
- Developing and implementing continuity plans including information security;
- Business continuity planning framework;
- Testing, maintaining and re-assessing business continuity plans;

It is suggested to every agency to follow ISO/IEC 27002 for preparing a robust and effective business continuity plan. And there must be indication of using that standard in the Information Security Policy document.

16. Monitoring & Improvement

It is important to monitor and review the information security policy for improvement. There are several phases of Information security strategy defined in section 7, monitoring is needed in every phase to improve service quality of that phase. The monitoring discussed here is

different from that is defined in Stage 6: Monitoring & Review in Section 7. This is the monitoring applicable on to the policy. The objective of this monitoring is to understand how the policy is implementing by the agency, what are the challenges or obstacles of implementation of the policy, what are the changes and actions required for improving the policy, whether any modification needed in the policy document because of any significant change in the information security context or in the management, etc.

There should be some direction in the policy document about monitoring (e.g. who will monitor, frequency of monitoring, whom to report the monitoring result, stakeholder consultation for improvement of the policy, etc).

17. National Cyber Security Strategy

It is important for an agency to be aware of the cyber security risk, threat and vulnerability of information as well. Beside this guideline a National Cyber Security Strategy needs to be formulated. Moreover, a separate agency may be established in future for addressing cyber security and information security issues and may be titled as “National Information Security Agency, Bangladesh (NISAB)”.

18. Appendix A: Template of Information Security Policy

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain:

a) A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
b) A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
c) A framework for setting control objectives and controls, including the structure of risk assessment and risk management;
d) A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
    1. Compliance with legislative, regulatory, and contractual requirements;
    2. Security education, training, and awareness requirements;
    3. Business continuity management;
    4. Consequences of information security policy violations;
e) A definition of general and specific responsibilities for information security management, including reporting information security incidents;
f) References to documents that may support the policy, e.g. guidelines and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader and users.

Sample Outline of an IS Policy:

I.	Preamble	IX.	Risk management
II.	Definitions	X.	Security Controls
III.	Introduction	XI.	Security policies, principles, standards, and Compliance
IV.	Purpose	XII.	Incident Management
V.	Scope	XIII.	Policy Awareness and Training on Information Security
VI.	Policy Governance & Monitoring	XIV.	Reference Documents (Guideline/Procedure/Appendix)
VII.	Information Asset and Classification		
VIII.	Roles & Responsibilities		

19. Appendix B: References

- CoBIT: IT Governance Framework
- ITIL: IT Services Management
- ISO/IEC 27000:2009, Information security management systems - Overview and vocabulary.
- ISO/IEC 27001:2005, Information security management systems - Requirements.
- ISO/IEC 27002:2005, Code of practice for information security management.
- ISO/IEC 27003, Information security management system implementation guidance.
- ISO/IEC 27004, Information security management - Measurement.
- ISO/IEC 27005:2008, Information security risk management.
- ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing.
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO 31000:2009 – Risk management - Principles and guidelines
- ISO/IEC TR 18044. Information technology- Security techniques- Information security incident management.

20. Appendix C: Acronyms

AS/NZS	Australia/New Zealand Standard
APT	Advanced Persistent Threat
BCC	Bangladesh Computer Council
BTRC	Bangladesh Telecommunication Regulatory Commission
CCA	Controller of Certifying Authorities
CoBIT	Control Objectives for Information and Related Technology
DDoS	Distributed Denial of Service
EU	European
FFIEC	Federal Financial Institutions Examination Council
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standards
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
OECD	Organization for Economic and Cooperation Development
PC	Personal Computer
PDCA	Plan-Do-Check-Act Cycle
PKI	Public Key Infrastructure
RFC	Request for Comment
USA	United States of America