ICT Risk Management Guideline

Bangladesh Krishi Bank

www.krishibank.org.bd

Risk Management Department
Head Office, 83-85 Motijheel C/A
Dhaka-1000
dgmrmd@krishibank.org.bd

মুখবন্ধ

বাংলাদেশ কৃষি ব্যাংক কৃষিঋণ বিতরণে দেশের রাষ্ট্র মালিকানাধীন সর্ববৃহৎ সরকারী বিশেষায়িত ব্যাংক। এ ব্যাংক বাংলাদেশের কৃষিসহ বিভিন্ন পেশায় নিয়োজিত ব্যক্তি/প্রতিষ্ঠানের আর্থসামাজিক উন্নয়নে অগ্রণী ভূমিকা পালন করে আসছে। ব্যাংকটি ১০৩৮টি শাখার মাধ্যমে আমানত সংগ্রহ, ঋণ বিতরণ, আমদানী রপ্তানী ব্যবসা, বৈদেশিক রেমিটেন্স প্রদান, Automated Chalan (এ চালান), RTGS, BFTN সেবাসহ সবধরণের ব্যাংকিং সেবা প্রদান করে আসছে। বর্তমানে বাংলাদেশ কৃষি ব্যাংকের সকল শাখায় অনলাইন সেবা চালু রয়েছে। ব্যাংকিং খাতে ৬ (ছয়)টি কোর Risk এর মধ্যে ICT Risk অন্যতম। অনলাইন সেবা চালু হবার পর বাংলাদেশ কৃষি ব্যাংকে Information & Communication Technology (ICT) এর গুরুত্ব এবং এ সংক্রান্ত ঝুঁকি ক্রমান্বয়ে বৃদ্ধি পাচ্ছে। ফলে ব্যাংকিং কার্যক্রমে ICT সংক্রান্ত ঝুঁকি চিহ্নিতকরণ, ঝুঁকি বিশ্লেষণ, ঝুঁকি মূল্যায়ন, ঝুঁকি নিয়ন্ত্রণ বা ঝুঁকি গ্রহণের বিষয়ে কাঠামোবদ্ধ সিদ্ধান্ত গ্রহণের জন্য বাংলাদেশ ব্যাংকের "Guideline on ICT Security for Banks and Non-Bank Financial Institutions" এর নির্দেশনার আলোকে বাংলাদেশ কৃষি ব্যাংক "ICT Risk Management Guideline-2022" প্রণয়ন করেছে। বাংলাদেশ ব্যাংকের বর্ণিত গাইডলাইনের নির্দেশনা যথাযথভাবে অনুসরণপূর্বক আইসিটি অপারেশন বিভাগ, বাংলাদেশ কৃষি ব্যাংক, প্রধান কার্যালয় কর্তৃক প্রয়োজনীয় সংযোজন, বিয়োজন, সংশোধন, পরিমার্জনপূর্বক চূড়ান্ত করা হয় এবং বিগত ৩১-১০-২০২২ তারিখে অনুষ্ঠিত বাংলাদেশ কৃষি ব্যাংক পরিচালনা পর্ষদের ৮১৭তম সভায় গাইডলাইনটি অনুমোদিত হয়। গাইডলাইনটি প্রণয়নের সাথে জড়িত সকল নির্বাহী ও কর্মকর্তাদের নিকট আমরা কৃতজ্ঞ। বাংলাদেশ কৃষি ব্যাংকের সকল স্তরের নিবাহী ও কর্মকর্তা/কর্মচারী এই গাইডলাইন দ্বারা উপকৃত হবেন এবং বাংলাদেশ কৃষি ব্যাংকের ICT Risk হ্রাস/প্রশমনে এ গাইডলাইনটি গুরুত্বপূর্ণ ভূমিকা রাখবে বলে আমরা আশাবাদী।

১৫.১১.২২

(মীর মোফাজ্জল হোসেন)
উপব্যবস্থাপনা পরিচালক
ও
প্রধান ঝুঁকি কর্মকর্তা (সিআরও)
বাংলাদেশ কৃষি ব্যাংক

Table of Contents

1.0 Introduction

This guideline is issued by Bangladesh Krishi Bank with a view to providing a structured way of identifying and analyzing potential risks in ICT and devising and implementing responses appropriate to their impact. These responses generally draw on strategies of risk prevention, risk transfer, impact mitigation or risk acceptance.

Risk management is a systematic process of identifying and assessing risks and taking actions to protect an organization against threats and vulnerabilities to align with its mission. These risks could stem from a wide variety of sources, including financial/technical uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.

As Bangladesh Krishi Bank (BKB) uses Information Technology (IT) systems to support its business operation successfully, Risk Management plays a critical role in protecting an organization's information assets.

1.1 Purpose

The Purpose of Risk Management is to identify potential issues before they occur so that risk-handling/Mitigation activities may be planned and invoked as needed across the whole information technology systems to help BKB better manage its IT-related risks.

In this document, we will assess the ICT risks for Information Technology Systems of BKB resulted by risk frequency (Likelihood) and consequences (Impact) based on Assets, Vulnerabilities and Threat Scenarios where vulnerabilities will be identified based on Key Risk Indicator (KRI) defined by Bangladesh Bank ICT Security Guidelines, PCI DSS and SWIFT etc. After assessing risk, we will determine the Business Continuity Planning (BCP) supported by Business Impact Analysis (BIA).

1.2 Scope

BKB having an aspiration to evolve as one of the best performing banks in the country is providing real-time core banking services to its customers through its branches, ATMs, POS, Third Party MFS and Banking Apps, other third party services such as bill collection of BTCL, DPDC, WASA, KDGCL, DESA, DESCO, Palli Bidyut Bill etc.

This ICT Risk Assessment Framework covers all the divisions/departments of Head Office and branches of BKB and business operation/services as well as all Information and Communication Technology (ICT) enabled systems that fall within the scope of the continuity planning are stated here. These are

i) People
   - I) Breach of internal guidelines , Policies & procedures
   - II) Breach of delegated authority
   - III) Criminal acts (Internal)
   - IV) Inadequate segregation of duties/dual controls
   - V) Inexperienced staff
   - VI) Staff oversight

ii) Process
   - I) Inadequate/inappropriate guidelines, policies & procedures
   - II) Inadequate/failure of communication
   - III) Inadequate reconciliation
   - IV) Poor software and Business Requirement Documentation
   - V) Inadequate security control
   - VI) Breach of regulatory & statutory provisions/requirements

VII) Inadequate change management process &
VIII) Inadequate contingency plan

iii) ICT Enabled Systems

However all the business operations of BKB are largely dependent on IT Systems and other infrastructure facilities. So up-keeping of IT System and other infrastructure facilities is a vital necessity for continuity of BKB's business. Major components of IT Systems are-

I) Core Banking Solutions (CBS)
II) BACH & BEFTN/RTGS /Automated Challan (A Challan)
III) Debit Card & National payment Switching of Bangladesh (NPBS) System.
IV) ATM, POS acquiring systems
V) ADC Apps Remittance Module
VI) Database (MS SQL Server, Oracle, MySQL)
VII) Server Network Devices & Security Appliances and related Hardware.
VIII) Network Infrastructure
IX) Application Software
X) System Software
XI) SWIFT Services
XII) System Up gradation/Update
XIII) System Migration
XIV) API with different Govt. and Non Govt. organization

iv) Other Infrastructures (Electrical, Power supplies and environmental)

v) External events
I) Criminal acts
II) Vendor miss-performance
III) Man-made disaster
IV) Natural disaster and
V) Political/legislative/regulatory causes

BKB has Data Center (DC). Data Center is located at the Head Office premises and DRS is located at BKB staff College , Mirpur , Dhaka, Bangladesh.

The critical phenomenon is to run business from DC or DRS during the time of disaster like fire, flood earthquake, cyclone, vandalism, cyber incident etc. Recovery of ICT Systems for continuity of business from DRS in case of any failure or disaster and coming to normal operation from DC is the major component of business continuity.

Similarly, any disaster may happen in the branch and at head office level which may disrupt the business operation locally or globally. So restoration of service and continuation of business in the branches is also within the scope of Risk Management.

1.3 Principles of Security

Confidentiality, Integrity and Availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of information security.
Confidentiality (C) - Is a set of rules that limits access to information.
Integrity (I) -Is the assurance that the information is trustworthy and accurate
Availability (A) - Is a guarantee of reliable access to the information by authorized people.

1.4 Component of Security

Information security consists of people. Process and technologies those are designed to protect individuals and organizations from cyber-crimes. Effective cyber Policy reduces the risk of a cyber-attack through the deliberate exploitation of systems networks and technologies. Effective and robust Information security requires an Information Security Management Systems (ISMS) should build on three components: **People, Processes and Technology.**

2.0 Risk Management

Risk means the uncertainty of future outcome or probability of adverse outcome from the system. Risk management refers to the practices of identifying potential risks in advance, analyzing them and taking precautionary steps to reduce the risk. It can be also defined that Risk Management is the process of assessing risk and then developing strategies to mitigate it. The Banking Risk Spectrum Defined by Bangladesh bank according to the BASEL Committee –

i) Assets Liability Management Risk
ii) Credit Risk Management
iii) Foreign Exchange Risk Management
iv) Money Laundering Prevention Risk (AML & CFT)
v) Internal Control and Compliance Risk
vi) Information Technology Risk
vii) Environmental & Social Risk Management

2.1 ICT Risk Possibilities area

ICT Risk are related to the following activities that are done all around the year for operational activities. Risk are related to the following activities that are done all around the year for operational activities.

i) Network Risk: Improper configuration, Authentication, device Malfunction failure Etc.
ii) Data Centre/Disaster Recovery Site Risk: Server Failure, Monitoring Failure etc.
iii) Hardware Risk: Power Faults, Equipment Incompatibilities, damage etc.
iv) Functionality Mismatch, Lack of proper security etc.
v) Internal, Regional and Global Cyber Threat- Phishing, Spoofing, DDoS, Malware, Spyware and other Cyber-criminal offences.

2.2 Risk governance, roles and responsibilities

Effective ICT risk management depends on appropriate governance and oversight. Risk oversight covers both the ICT risk management process as well as individual accountabilities for managing ICT risk outcomes.

2.2.1 Roles of Board of Directors (BoDs).

According to the BASEL Committee for Banking Supervision (BCBs) there are some principles regarding the roles and responsibilities of the BoDs.

I) The board of directors should take the lead the establishing a strong risk management culture. The board of directors and seniors management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standard and incentives for professional and responsible behavior.

II) The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decisions.

III) The board of directors should approve and review a ICT risk appetite and tolerance statement for ICT operation risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.

2.2.2 Roles and Responsibilities of Top Management

I) Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, process and systems consistent with the risk appetite and tolerance.

II) Senior management should ensure the identification and assessment of the ICT operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

III) Senior management should ensure that there is an approval process for all new products, activities, process and systems that fully assesses ICT operational risk.

IV) Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place be in place at the board, senior management and business line levels that support proactive management of ICT operational risk.

2.2.3 Roles of RMD

I) All ICT enabled systems, services; Hardware should be handled carefully to mitigate risk.

II) The employee should follow internal use their delegated power during ICT operation.

III) The employee should follow internal and external policies, procedures and guidelines carefully.

IV) There should be dual control/segregation of duties in all ICT related activities.

V) All employee should have clear understanding about their roles and responsibilities and should not engage with any internal or external ICT related Crimes.

VI) There should be staff turnover and all employee should have expertise to do their related ICT activities.

2.2.4 Three Lines Defense model

BKB has 3 lines of Defense model that has been used to clearly define risk management roles and responsibilities: ICT Operational Risk Management Framework

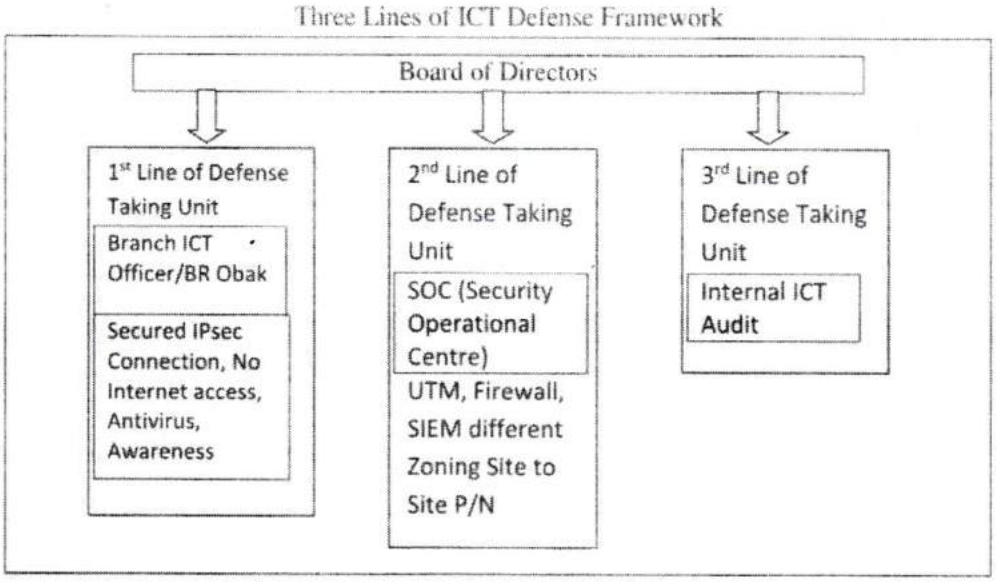

Figure: 1

The bank shall deploy this defensive approach for management of ICT risk associate in ICT assets.

3.0 ICT Risk Management Process

The process of risk management is an ongoing process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. The choice of countermeasures (Controls) used to manage risks must a balance between productivity, cost, effectiveness of the countermeasures and the value of the informational asset being protected.

The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation and risk monitoring and review.

3.1 Context Establishment

It means understand the organization's objectives, defining internal and external factors that could be a source of uncertainty, helping identify risk and setting the scope and risk criteria for the remaining risk management process. Establishing the context is the starting point to the development of the risk management process. If this step is done poorly it will impact the value of the rest of the process and will lead to an unreliable assessment of risk and possibly the section of inappropriate controls.

There are approaches for establishing the context of the risk assessment process and breaks it into three elements:

i) Establishing the external context within which the organizational operates.
ii) Establishing the internal context of the organization.
iii) Establishing the security risk management context for the organization

Management will define and Risk Assessment Team will monitor the internal and external context of BKB'S ICT assets

3.2 Risk Assessment

All the risks are related to some assets, likelihood and impacts. And identification of assets is the primary step for risk identification.

The risk management process can be applied to the bank as a whole any discrete part of the organization (e.g. a department/division, a physical location, a service), any information system, existing planned or particular aspects of control (e.g. business continuity planning).

3.2.1 Risk Assessments Process

Any assessment should have methodology to define and assess. Methodology is a systematic analysis of methods applied to prepare any framework. So ICT Risk management also should have a methodology. As there are many Standard, Frameworks (e.g. OCTAVE, ISO 27005 and NIST SP 800-30 etc) And Guidelines. We have followed here standard: ISO /IEC 27005:2011 for BKB ICT Risk Management. A High level view of the risk management process is specified in ISO 31000 and shown in Figure: 2.

The Risk Management process:-

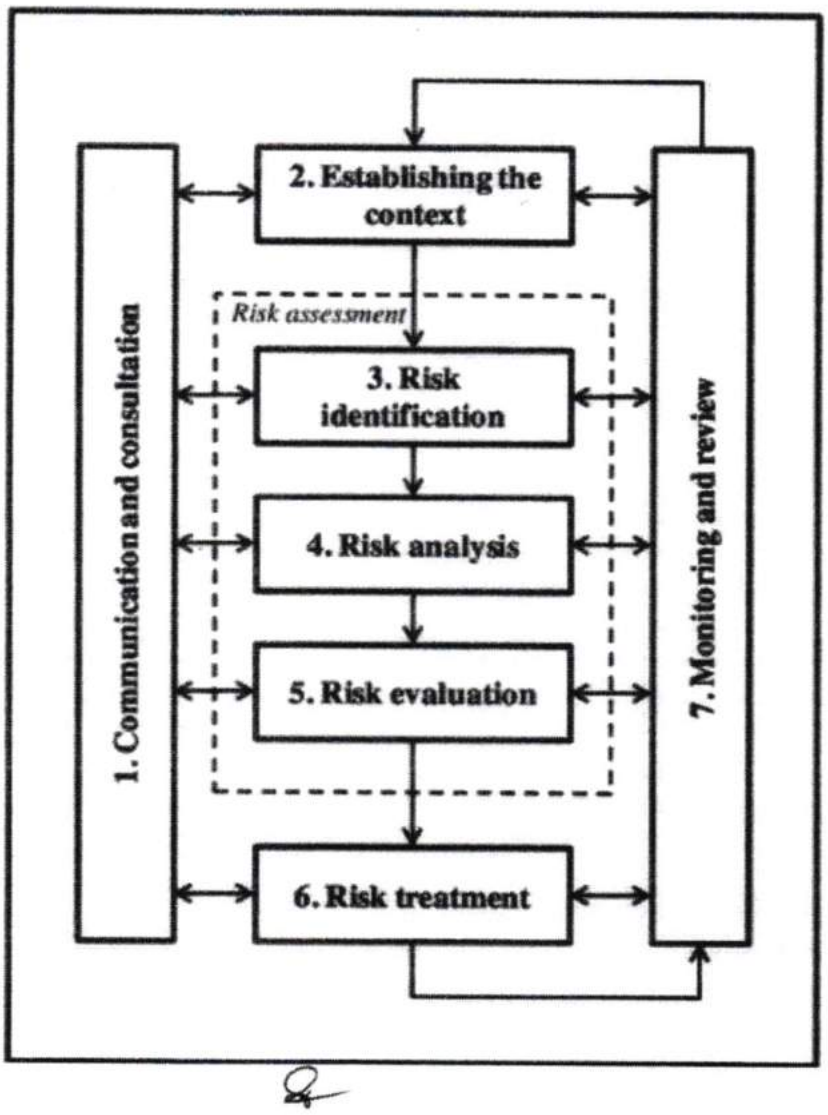

Figure: 2

3.2.2 **Identification of Assets**

The ICT asset is valued in terms of the impact of total loss of the asset in terms of Confidentiality, Integrity or Availability

Table: 1

Criticality Rating	Risk Description & Necessary Actions	
High	The loss of Confidentiality (C), Integrity (I), or Availability (A) could be expected to have severe or catastrophic adverse effect on organization operations, organizational assets or individuals.	
Medium	The loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	
Low	The loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	

3.2.3 **List of Identified Asset**

BKB shall categories its ICT assets according to the Types and criticality to participate them in the risk management process. There is large number of activities related with ICT operation in banks. These ICT enabled Assets are described and listed in APPENDIX-1 with their criticality. The Bank shall identify ICT enabled assets which has minimum risk associate in the banking operation.

3.2.4 Identification of Key Risk Indicator (KRI)

A key risk indicator (KRI) is a measure used in management to indicate how risky an activity is. Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. Here the key risk indicator KRI) has been identified based on Bangladesh Bank ICT Security Guideline, PCI DSS and SWIFT etc. These are most powerful indicator to assess ICT risk in the bank. The bank shall identify its key risk indicator according to the list described in the APENDIX-2.

3.2.5 Identification of Risk-Scenarios

Treats are ubiquitous (any time anywhere) and represent possible sources of negative impact to an organization. Threats can be natural, environmental, social, technical and medical and can lead to disruptions in operations which can adversely impact an organization. Threat categories and sources are interrelated with Risk Scenarios. The risk Scenarios are very essential to calculate ICT risk of the banks. BKB shall classify all of ICT related Threat category and sources along with their Risk Scenarios according to the prescribed form which has been listed in the APENDIX-3.

3.2.6 **Risk Appetite and Risk Tolerance**

Risk Appetite is the amount of risk that an organization is willing to accept in the pursuit of its business objectives and outcomes. It represents an organization's attitude particular risks, and takes consideration the expectations of key stakeholders such as owner customers' third-party providers' staff and the public. Executive level of Management shall identify what are acceptable levels of residual risk. Risk appetite may change over time as new information and outcomes become available and as shareholder expectation evolve.

Risk tolerance can be defined as the acceptable variance from the organization's risk appetite. Bank/Board of Directors shall determine acceptable tolerance limits and whether they the negotiable.

There is an interrelation between Threat sources, Risk Scenarios, Risk Appetite and Risk Tolerance for calculation of ICT risk of the bank. There is a list of threat-sources, Risk scenarios, risk appetite and risk tolerance which have been defined by BKB to mitigate its risk exposures. The approved list of Risk Appetite and Risk Tolerance is detailed out in the bank shall apply this APENDIX-4 for calculating ICT risk of the IT assets.

3.2.7 Relationship between Vulnerabilities and Risk Scenarios based on Assets

Vulnerability is the weakness of assets which can be exploited by a threat Actor, such as an attacker to perform unauthorized actions within a computer system. These unauthorized actions are the Risk Scenarios that Bank might face. There is a relationship between Vulnerabilities and Risk Scenarios aligned with Asset which has been described in the APENDIX-5.

3.2.8 Risk Frequency Evaluation

Risk frequency may be defined in terms of the chance (Likelihood).

Measure of risk frequency evaluation

Likelihood – chance of the risk happening/Occurrence.
Likelihood Scale

Risk Likelihood Rating Definition is on table

Table: 2

Rating	Likelihood	Likelihood of Occurrence
0.1	Low	Not expected, but there's slight Possibility it may occur at some time.
0.5	Moderate	The event might occur at some time as there is a history of casual occurrence
1	High	There is strong possibility the event will occur as there is a history of frequent.

BKB shall determine relationship between Vulnerabilities and Risk Frequency rating along with Risk Scenarios which has been listed in the APENDIX-6.

3.2.9 Risk Analysis

To identify the likelihood of compromises of confidentiality, integrity and availability to people, process and technology by considering different threat scenarios. This will also involve interviews with delegated staff such as business owner, Human Resources, Datacenter Premises, information (Data) owner, Core Application Software owner, Critical System Software owner, Databases owner, Hardware/Storage owner, Network Equipment and Communication Link owner who are responsible for the security of the people, Process and technology on behalf of the owners.

Measure the size & importance of risk

Impact = the amount of loss or damage if the happened
Likelihood x impact = level of risk (Risk score)/ measurement

Having identified the risks involved, they need to be assessed or measured in terms of the chance they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk

associated with an event is a combination of the chance (Likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

Therefore, each risk element can be rated by:

The chance of the risk happening –"Likelihood"
The amount of loss or damage if the risk happened-'impact' (consequence)

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood and impact and from these get a level of risk score using the risk measurement.

3.2.10 Impact Scale

The impact is the amount of loss or damage if the risk happened in the ICT Assets. BKB shall define risk impact on ICT Assets based on the Rating defined bellow:

Table: 3

Rating	Magnitude of Impact	Impact Definition
100	High	Occurrence of the risk 1.May result in stoppage of the service for BKB's customer or serious disruption of service: 2.May result in the loss of resources or sensitive data ; or may significantly harm, or 3.impede the BKB's mission reputation or interest
50	Moderate	Occurrence of the risk 1..May result disruption of service for the client or users 2.May increase customer dissatisfaction; or 3.May violate, harm the BKB's mission, reputation or interest
10	Low	Occurrence of the risk 1.May result disruption of service for certain area of service or the branch or sometimes; 2.May noticeably affect the BKB's mission, reputation or interest

3.2.11 Overall Risk Rating Table

The overall risk rating of the bank shall show the risk grade of the bank ICT Assets. This overall risk rating shall be the key for calculating the Bank's final risk rating along with Risk grade which has been illustrated in the APENDIX-7. The table in APENDIX-7 shows the frequency (Likelihood) and consequences (Impact) have been assessed for the bank.

3.2.12 Risk Determination

The Risk Determination shall be calculated based on the impact scale rating with magnitude as described earlier. The following table given below is used to determine overall risk rating.

Table: 4

Risk Likelihood	Risk Impact		
	Low(10)	Moderate (50)	High (100)
H(1.0)	L 10 x1.0=10	M 50 x1.0=50	H 100 x1.0=100
M(0.5)	L 10 x0.5=5	M 50 x0.5=25	M 100 x0.5=50
L(0.1)	L 10 x0.1=1	L 50 x0.1=5	L 100 x0.1=10

3.2.13 Risk Scale

L (1 to 10)
M (> 10 to 50)
H (>50 to 100)

3.2.14 Risk rating and parameters

Risk rating performed in determining the impact and likelihood of occurrence of the risk. Risk rating should be rated after taking consideration of the controls in place.

Rating should consider the range of potential impact and how likely these would occur. Where risk impacts different risk factors, the greater rating will be used. For example if a minor fraud event occurs, the financial impact may be insignificant in terms of taka value but the impact to reputation and bank image would be major if the fraud was due to laps of fundamental controls. Thus impact of the risk should be major.

Risk is to be assessed by considering estimates of:

1) Impact (qualitative/quantitative) which measures the expected effect of a risk once it has occurred.

2) Likelihood which measures the expected frequency of a risk occurring or materializing taking into consideration current control or risk treatment in place.

Using scales of likelihood and impact within a risk matrix will allow us to combine the two separate measures to generate a matrix of risk scores.

Likelihood x impact = level of risk (Risk score)/ measurement

3.2.15 Overall Risk Rating Matrix and Calculation

The following table shows the overall risk rating with the calculated risk value as condition.

Table: 5

Overall Risk Rating		
Rate	Value	Condition
Strong	1	If the percentage is below 8%
Satisfactory	2	If the percentage is below or equal 15% and above or equal 8%
Fair	3	If the percentage is below or equal 25% and above 15%

Marginal	4	If the percentage is below or equal 30% and above 25%
Unsatisfactory	5	above 30%

3.2.16 Finalization of ICT Risk Rating Calculation

The bank shall finalize its risk rating with grade value according to the table 6. These value shall be calculated based on the value of APENDIX-7 and table 4 as described.

Table: 6

Risk Criticality	Risk Scale	Number of risk Criticality	Risk Calculation Matrix	Overall Calculation
High (H)	>50 to 100	0	0	0
Medium (M)	>10 to 50	7	4 x 50	200
			3 x 25	75
Low (L)	1 to 10	52	41 x 10	410
			9 x 5	45
			2 x 1	2
Total				732
Overall Risk Rating Calculation = (732/5900)*100				**12.41%**

Remarks: The overall Risk grade is 12.41% which defines that risk level is **Satisfactory**.

4.0 Management Action Trigger (MAT) Policy

Management Action Trigger (MAT) is the trigger levels to warn persistently unaddressed high risk area in information technology that may cause severe disruption in business continuity. It defines management's tolerance acceptance level in a specific area. When these levels or limits are breached, management should be consulted to determine the next course of action to be adopted as specified in BCP and DR Plan.

4.1 Classification of Risk Triggers

Based upon the risk assessment result, some risks will require a response in the existing set up some will only require a response in the monitoring system and some will not require any response at all. If a risk is deemed to be high or overall risk rating degrades below satisfactory level, it needs response with high alacrity and escalation to the top management in cases. Response to negative risks, treat are one or a combination of following 6 (six) triggers.

1. **Avoid**: When there is no possibility for the risk to occur because the infrastructure is never susceptible to that type of risk.
2. **Mitigate**: When the risk occurs it will only have minor effect because the threat has been anticipated and provision for addressing it are in place.
3. **Transfer**: The risk involves participation of third party so that the third party assumes responsibility for addressing portion of the risk impact.
4. **Accept:** The risk is so insignificant or the risk is so improbable that no change is needed.
5. **Contingency Plan:** Although a trigger is established that will provide notice that an opportunity is now available to improve on one or more of the project objectives.
6. **Management Action**: The risk is severe and requires urgent involvement of Management actions. It is this point the Management Action Trigger (MAT) has to be activated. The incident will be escalated to the next level in the organization structure if the risk is not mitigated immediately.

A) In case the relevant wings have failed to resolve the problem it will then be escalated to ICT Security Committee an ICT Risk Management Committee and the reporting executive i.e. Managing Director & CEO . At the same time, the CRO will be updated about the Risk.

B) The MD & CEO in turn will review the impact of the risk and decide accordingly.

4.2 Risk Management Strategy

BKB shall follow four standard risk management strategies to manage ICT risk. The best choice shall depend on the nature of the specific risk and the bank's overall situation.

Table: 7

High Frequency	HF+LM (Manage Strategy)	HF+HM (Avoid Strategy)
Low Frequency	LF+LM (Accept Strategy)	LF+HM (Transfer Strategy)
	Low Magnitude	**High Magnitude**

4.2.1 Manage Strategy

* If there is high frequency but low magnitude of the risk effect then the risk shall be managed.

4.2.2 Accept Strategy

* If there is low frequency but low magnitude of the risk's effect then the risk shall be accepted.

* If the risk is in the level of tolerance and loss is minimum then it shall be accepted.

4.2.3 Transfer Strategy

* If there is low frequency but high magnitude of the risk's effect then the risk shall be transferred.

4.2.4 Avoid Strategy

* If there is high frequency and high magnitude of the risk's effect then the risk shall be avoid.

4.3 Monitoring and reviewing

Risk need to be monitoring periodically to ensure changing circumstances do not alter the risk priorities. Regular monitoring activities help quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. It is natural that very few risks will remain static. Therefore the risk management process needs to be regularly repeated, so that new risks are captured in the process and effectively managed. Risk management plan shall be reviewed at least on an annual basis. An effective way to ensure that is to combine risk planning or risk review with annual business planning.

4.4 Risk Mitigation

Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled, e.g. natural disasters. Risk mitigation tools or programs are used to reduce the exposure to, or frequency and/or severity of such events. Mitigation tools or programs are used to reduce the exposure to, or frequency and/or severity of such events. Mitigation tools like DRP, BCP, Back up monitoring, segregation of duties, change management, Patch Management, high Availability of hardware and software resources and other control system shall be developed and deployed.

4.5 Risk Reporting

After proper analysis risks are to be prioritized and reported to competent authorities (both internal and external). Bank Prepares Monthly ICT Management Report (MRMR on ICT) and comprehensive Risk Management Report (CRMR) according to the formats provided by BKB as a minimum

requirement. Bank arranges monthly meeting of ERMC (Executive Risk Management Committee) to discuss the risk based on the findings of the risk reports and submit the CRMR and MRMR along with the minutes of ERMC meeting to DOS of BB within stipulated time.

Discussions, decisions of ERMC must be reflects in the meeting minutes. Bank also submits the board approved Risk Appetite Statement (RAS) on yearly basis and BRMC meeting minutes on regular basis. Besides Bank submits a soft copy of Stress Test report to DOS of BB on half yearly basis along with risk report. The risk reports and forwarding letter sent to BB are signed by the CRO.

In addition, bank shall submit review report (board resolution copy) of Risk Management Policies and effectiveness of risk management functions with the approval of the directors to DOS of BB on yearly basis.

5.0 Reward & Punishment

For promoting compliance culture among the departments, units and branches of BKB the rewarding system will be as follows:

1) The Department, Unit and Branch that will achieve Strong Risk Assessment Rating will be awarded as " Most Compliant Division, Unit and Branch for the year respectively"
2) In addition of the above, the first three lowest point achievers having Satisfactory rating may be awarded as "First, second and Third Compliant Division, Unit and Branch of the year" respectively.

However alternatively for poor performance in risk Assessment Rating, following disciplinary action will be applicable.

*If any Division/Branch gets Marginal rating on ICT Risk Assessment, respective Division Head/Branch Manager (BM) will get warning /caution letter immediately.

Within 90 days of sending mentioned Marginal Risk Assessment rating, a review Risk Assessment will be conducted to find out any improvement of the Division/Branch/Unit. With necessary administrative action.

If any Division /Branch/Unit gets Marginal rating in Risk Assessment, after consultation with MD & CEO will determine the extent of administrative action against the Division/Unit Head /Concern person. Within 90 days of sending Risk Assessment rating, a review Risk Assessment will be conducted to find out any improvement of the Division/Branch/Unit.

If bank's employee willfully/knowingly furnishes false information in reporting to BB, Such an offence is punishable under section 109(2) of the Bank Company Act 1991. BB may impose penalty as per section 109 (7) of the said Act if bank fails to submit the above mentioned reports within stipulated time without any acceptable/satisfactory reason.

6.0 Conclusion

To maintain the continuance of this assessment, It Division has taken the responsibility to assess the risk for every year. In this assessment, the department has made significant changes from the earlier risk assessment process to meet the compliance issues of Bangladesh Bank, SWIFT, PCI DSS, and ISO etc.

Here assets have been identified with criticality based on CIA. Also relationship has been aligned among assets, Vulnerabilities, Threat-Sources and Risk Scenarios. In addition, Risk Likelihood have been measured based on both assets and their evaluation on Risk Scenarios. Then, impacts of risks have been enumerated the based on impact scale. Subsequently, overall Risk Assessment Rating has been found according to Risk Assessment Framework defined by BKB.

For the Risk Scenarios, It will be adjusted with Business Impact Analysis (BIA) and Business Continuity Planning (BCP) have also been assessed having discussed with all stakeholders. This assessment will not only Provide a Rating only but also define a clear notion for prevention, detection and treatment of an incident.

7.0 Maintain and Review

* The BKB ICT Risk Management Framework shall be updated at least annually with the approval of Management Coordinating Committee (MCC), Risk Management Committee (RMC) and BKB Board of Directors.
* The risk appetite, risk tolerance and risk frequency shall be updated at least annually with the approval of Management Coordinating Committee (MCC), Risk Management Committee (RMC) and BKB Board of Directors.
* If any changes are required any time, it shall be updated by the approval of Management Coordinating Committee (MCC), Risk Management Committee (RMC) and BKB Board of Directors.
*When any changes shall be done, it shall be sent to all branches, regional offices and departments of BKB.

APENDIX-1: Identification of Assets with their criticality

SL.	Asset Type/ Category	Particulars	Criticality
1.	Core Application Software	Core Banking System	H
		Banking App	H
		BACH-BEFTN Management Software	H
		BACH-BACPS Management Software	H
		Card issuing, Authorizations & Switching System	H
		Bangladesh Krishi Bank Website	H
		Internet Banking	H
		SWIFT Alliance Access, SWIFT Access Gateway	H
		Real Time Gross Settlement System (RTGS)	H
		Third Party integrated applications	H
		Remittance applications system	H
		Email system (External/Internal)	H
		Messaging Gateway	H
2.	End-User Application Software	Browser	M
		Bangla Typing Software	M
		Compressed Software: WinRAR, WinZip	M
		MS Office: 2003, 2007, 2010, 2013, 2016	M
		Photo viewer and editor: ACDSEE	L
		PDF Reader: Foxit Reader, Adobe Acrobat	M
		Remote Network Connectivity tools	H
		Database connectivity tools	H
3.	Internet Applications		
		HR Management System	M
		Integrated on-line MIS (Affairs, Income, Expenditure)	M
		Web Based MIS (WMIS)	H
		Inventory Management System	M
		All Loan, CL Process and Recovery	H
		On-line Remittance Payment Software (BKB Remit)	H
		CTR/ STR Reporting Software (Go AML)	H
		Reconciliation Management System	H
		PF Online System	H
		BTCL Bill Collection Software	H
		Loan Collateral/ Security Information System	H
		Online CIB Submission	H
		KGDCL Bill collection Software	M
		SGCL Bill Collection Software	M
4.	Database	CBS Database (Customer data and Financial Data)	H
		Card Database	H
		HR Database	H
5.	Storage	Server Storage	H
		SAN Storage	H
		Individual PC Storage	H
		SWIFT Storage	H
		Tape Storage	H
6.	Information (Data)	Sensitive data of different devices (Passwords, configurations)	H
		Source code of software	H
		System documentation	H

		Intellectual property	H
		Network infrastructure design	H
		Network or any other encryption Key	H
		Strategic plans	M
		Any log files of any devices	H
7.	Network Equipment	Core Routers	H
		Core Switches	H
		Core Firewalls (IDS/IPS)	H
		Load Balancer	H
		DC server Firm Switches	H
		Open Wi-Fi	H
		Branch Routers	H
		Data & Power cable in same Channel	H
		Branch Switches	M
		ATM Routers	M
		Unstructured LAN/ Structured LAN	M
		Unstructured Power Cable	M
		Wireless Access Controller	L
		SAN Switches	M
		Network Rack	L
		Lack of proper documentation of al l connected routers, switches and servers (With Design)	M
		Unauthorized Wi-Fi in Office area	H
SL.	Asset Type/ Category	Particulars	Criticality
8.	Security Equipment	Improper maintaining log and backup	H
		License expired	H
		Patch nor Updated	H
		Action not taken regarding Alarm	H
9.	Operating System Software	Unlicensed Operating System	H
		Critical debugging Error	H
		File Mismatch	H
		Microsoft Exchange System	H
		Domain Naming System (DNS)	H
		MS Active Directory (AD)	H
		Anti-Virus-Sophos End- Point Security etc.	H
		Microsoft Hyper-V:2008, 2012 and 2016	H
		VMware vSphere	H
		Patch Management System (WSUS)	H
		Environmental Management System	M
10.	Hardware System	Desktop computers	H
		Servers	H
		Laptops	L
		Hardware Security Module (HSM)	H
		ATM Machine	M
		Alarm Systems	M
		Access Control Systems (Physical)	M
		Printers	L
		MICR Scanners	H
		Document Scanners	L
		Removable Media	L
		Modem for Branch	M

		UPS, Online UPS	H
11.	Datacenter Premises	Entrance to the DC	H
		Fire Protection System	H
		Cooling System with backup unit	H
		Power Distribution System (PDU)	H
		Water Leakage precaution and Drainage system	H
		Humidity Controller	H
		EMS	H
		Alarm System	H
		Proper Distance for server rack	H
		UPS Backup System	H
		Emergency Exit System	H
		Emergency Supply of any equipment for DC	H
		Change Management log (Physical or logical)	H
		Proper Cabling for Data and Power with Marking	H
		PAC	H
SL	Asset Type/ Category	Particulars	Criticality
12.	Human Resources (People)	**Decision Maker:** Top Management, Project Leader	H
		End-users: Human resources management, Financial management, Risk manager	H
		Operation/ Maintenance Staff: Departmental employees system administrator, database administrator, Network administrator, Help Desk, application deployment operator, Physical Security officers, IT Security officers	H
		Application developers	M
		Subject matter experts	M
13.	Datacenter Supporting Equipment	Electrical Systems e.g. Power Supply, Generator	H
		Water Supply & Drainage Systems	H
		Precession Air Controller	H
		Fire Extinguisher	H
		Telephone line PABX, PBX, Internal telephone networks	L

APENDIX-2: Key Risk Indicator (KRI)

SL	Key Risk Indicator (KRI)	Policy, Guidelines, Framework		
		Bangladesh Bank	SWIFT	PCI DSS
1	Authentication token/password theft/misconfigured	5.2.12,5.3.4 5.4.2, 5.7.21	5.2 4.2	6.5.8,8.1 (8.1.1-8), 8.2(8.2.1-9), 8.3
2	Deletion of logs and forensic evidence	5.2.12, 6.1.7 6.3.3	1.2	10.1,10.2
3	Privilege access management	5.4.1,6.4.1	1.2,5.1	7.1, 7.2
4	Exploitation of insecure system configuration/ misconfiguration		2.3	1.1, 1.2
5	Loss of data integrity	9.2.4, 9.3.1	2.1, 2.4A, 6.3	4.1, 10.5.5,11.5
6	Compromise of trusted backup data	7.3	2.5A	9.5 9.6
7	Execution of malicious	5.2.9	6.1	6.4 6.5.2
8	Segregation of duty violations	2.3.4	5.1	10.5(10.5.1-4), 6.4.2
9	Unauthorized system changes	4.1.1	1.2, 6.2	10.5.2, 10.5.5, 10.6, 10.6.3
10	Missing of security update and critical patch/updates regularly	5.4.9 (b)	2.2AB	5.2, 6.2
11	Increase security risk from improperly trained and unaware staff	2.7	7.2	6.5 9.9.3, 12.6
12	No High availability	8.3.3		
13	Undefined/Inactive/Concurrent Session	9.2.6	2.6A	1.3.5, 6.5.10
14	NTP not configured			10.4
15	Mix environment (Test, development and production)	8.5.2	1.1A	2.2.1, 6.4.1
16	Firewall/IPS/IDS/WAF/ESA not enabled/incorporated	5.7.8	2.3AB	1.1, 1.1.4, 1.2.3, 11.4
17	System not Licensed	8.5.1		
18	Traffic/Data/System Confidentiality	5.2.3, 5.11.3, 7.3.7	2.1, 2.4A 2.5A	2.3, 3.4
19	Unprotected storage/removable media	5.2.5	3.1AB	3.4
20	Unnecessary Programs/services	5.4.7	2.3AB	2.1, 2.2.5, 6.4.6
21	No middleware/application		2.4A	
22	No Operation documentation and procedure (for user and administrator) Prepared for system/software	8.3.7, 8.4		3.6
23	Application weakness, no input validation and error handing	8.5.5		6.5.8
24	Disaster (Manmade or natural) medical and environment issues	7.1, 7.2		
25	No proper security monitoring logs and events	9.2.7	6.4AB	10.5.5, 11.4

APENDIX-3: Relation between Threat Source and Risk Scenarios

Threat category	Threat-sources	Risk Scenarios
Human	Acts of human error or failure	Accidents, Disclosure of passwords and Sensitive Information
Technical	Technology Obsolescence	Antiquated or outdated technologies
	Technical software failures or errors	Software failure (System, OS, database etc.)
	Technical hardware failures or errors	Hardware/Disk malfunction/failure/damage
	Deviation in quality of service from service provides	Communication link down, Damage caused by service provider
Cyber –attack activities	Deliberate cyber-attack activities	Malicious code inject by insider or outsider
		Distributed Denial of Service
		Social engineering
		Disclosure of sensitive information
		Cyber-crime/attack
		Compromising confidential information
		Unauthorized access to information system
		Corruption of data
		Theft
Forces of nature	Natural Disaster	Food
		Fire
		Earthquakes
		Lightning
		Supply Shortage
		Communications services breakdown
		Power failure
	Environmental	Long-term power failure
		Pollution
	Medical	Epidemiology
		Pandemic FLU
		Dengue Fever
		Health & Safety regulations
Geographical	Social	Mass Behavior
		Human intervention
		Disgruntled Employee
		Employee morale
	Political	Political Spying

APENDIX-4: Risk Appetite and Risk Tolerance Level

Threat-sources	Risk Scenarios	Risk Appetite	Risk Tolerance
Acts of human error or failure	Disclosure passwords	15	± 20%
	Disclosure of Critical Information	10	
	Disclosure of Source Code	15	
	Inability or Limited ability to perform missions/business functions	20	± 30%
	Delay of projects finalization	10	± 30%
Technology obsolescence	System Unavailable	2	± 10%
Technical software and Database failures or errors	System Software Failure	5	± 20%
Technical hardware failures or errors	Hardware/Disk malfunction/failure/damage	5	± 20%
Deviation in quality of service from service providers	Communications link down,	5	± 20%
	Damage caused by service provider		
	Delay of equipment supply and services		
Deliberate cyber-attack activities	System Compromised	10	± 0%
	Denial of Service	2	± 0%
	Disclosure of sensitive information	10	± 0%
	Cyber Crime/attack	25	± 0%
	Data Theft	5	± 0%
	Unauthorized access to information system	2	± 0%
	Corruption of Banking data	10	± 0%
	Social Engineering		
Natural Disaster	Food	1	± 10%
	Fire	1	± 10%
	Earthquakes	1	± 10%
	Lightning	2	± 10%
	Supply Shortage	5	± 30%
	Communications services breakdown	50	± 20%
	Power failure	10	± 30%
Environmental	Long-term power failure	1	± 30%
	Inadequate environment in the DC,DRS and Data processing area	5	± 30%
	Inadequate cooling system	1	
Medical (Health safety)	Epidemiology	10	± 30%
	Pandemic Flu		
	Dengue Fever		
	Pandemic Flu		
	Health and safety Failure		

APENDIX-5: Relation between Vulnerability and Risk Scenarios

SL	Assets	Vulnerabilities	Risk Scenarios
1.	Core Application	1. Well-known flaws in the software. 2. Unauthorized system changes.	Software Failure
		1. Exploitation of insecure system configuration/ miss configuration. 2. Unnecessary program/ services. 3. Antiquated or outdated technologies.	Hardware failure/ damages
		1. No Account session limiting network security devices.	Denial of Services (DoS/DDoS)
		1. Operating Systems and security patches are not updated. 2. Internet access from server. 3. Brower Application is not update with latest security patches.	Unauthorized access to information system, Social engineering, Theft
		1. Due to Unauthorized software, users are not aware of safe browsing policy.	Compromising confidential information
		1.Application weakness 2.No input validation 3.Developers are not maintaining SDLC framework 4. Antiquated or outdated technologies.	Malicious code inject by insider or outsider
		1.User intends to write down the password due to password complexity Policy/ long character password.	Disclosure of Passwords
		1. Lack of user awareness. 2.Firewall/IPS/IDS/WAF not enabled/ Incorporated.	Social engineering
		1.No Operational documentation and procedure (for user and administrator) Prepared for Application/ software.	Inability or limited ability to perform missions/business functions, Delay of projects.
		1. Backup is not properly taken. 2. No high Availability	System unavailable.
		1.No encryption	Disclosure of sensitive information
2.	End-User Application Software	1. Well-known flaws in the software.	Software failure
		2.No security patch	Cyber Crime/ Attack
3.	In-house developed Applications	1. Applying application programs to the wrong data in terms of time.	Software failure
		2. Well-known flaws in the software. 3. There is no standard secured coding. 4. Application security is not properly maintained. 5. SDLC is not followed.	Cyber Crime/ Attack
4.	Databases	1. No high Availability.	Databases Software failure
		1. Power failure, No redundant on storage media. 2. No high Availability.	System failure.

SL	**Assets**	**Vulnerabilities**	**Risk Scenarios**
		1. Application weakness, No input validation. 2. Unwanted open ports. 3. Internet access from server. 4. Data query is not programmatic.	Malicious code injects by insider or outsider.
		1. Clear text password is stored on database.	Disclosure of passwords.
		1. Database Systems security patch is not updated. 2. Internet access from server.	Unauthorized access to information system, Theft
		1. Backup is not properly taken. 2. No high Availability.	System unavailable.
		1.No encryption	Disclosure of sensitive information.
5.	Storages	1. Faulty installation of storage media. 2. Insufficient maintenance. 3. Lack of periodic replacement. 4. Unprotected storage.	Power failure.
			Disk Failure.
			Hardware malfunction
			Software failure
			Unauthorized access to information system
		1. Backup is not properly taken. 2. No high Availability.	System unavailable.
		1.No proper security monitoring (logs and events)	Cyber Crime/ Attack Malicious code injects by insider or outsider.
		1.No encryption	Disclosure of sensitive information.
6.	Information (Data)	1. Due to Unauthorized software. 2. Users are not aware of safe browsing policy. 3. Operating system and security patch is not updated 4. Due to unauthorized software 5. Anti-virus not updated. 6. Unrestricted remote excess	Cyber Crime/ Attack
		1.Lack of physical security 2. Makes environment (Test. Development and production)	Theft
		1.Applying application programs to the wrong data 2. Well-known flaws in the software. 3. Power failure 4. No redundant on storage media	Hardware/software failure
		1.Lose of data integrity 2. Unnecessary program/services	Corruption of data
		1.Cause of disaster (Manmade or natural)	Communications services breakdown
		1.Backup is not properly taken	System unavailable
		1.No encryption	Disclosure of sensitive information

SL	Assets	Vulnerabilities	Risk Scenarios
7	Network equipment's	1.Unprotected communications lines 2. Unprotected sensitive traffic 3. Poor joint cabling 4. Single point of failure 5. Insecure network architecture 6. Inadequate network management (Resilience of routing) 7. Firewall/ IPS/IDS/WAF not enabled/incorporated 8. NTP not configured 9. Unwanted open ports 10. Unused user accounts 11. No encryptions 12. Antiquated or outdated technologies	Disclosure of sensitive information Hardware malfunction/failure Communication link down Cybercrime/attack Power failure Evidence missing/Forensic issue after any occurrence
8	Operating System Software	1.Operating system security patch are not updated 2. Well-known flaws in the software	Cybercrime/attack
9	Hardware systems	1.Susceptibility to humidity, dust, soiling 2. Sensitivity to electromagnetic radiation 3. Susceptibility to voltage variation 4. Susceptibility to temperature variations 5. Lightening 6.Antiquated or outdated technologies	Hardware malfunction/ failure Power failure Unauthorized access to information system
10	Data center premises	1.Low height of ground floor 2. All the walls are not fire resistant 3. Brick built, high earthquake prone area, can't survive for earthquake of Richter scale 6.0 and beyond 4. Brick built; glass built 5. Pollution	Flood Fire (Burning) Earthquakes Long term power failure
11	Human resources (people)	1.Aggresive, anger and resentment 2. arrogant 3. Insecurity 4. Naive, short sighted 5. Low employee morale 6. Mass behavior	Disgruntled employee Political spying Human intervention -Pandemic flow -Dengue fever
12	Data center supporting equipment	1. Redundancy is not present on Power supply water supply & drainage systems, and Air Controller 2. Short circuit on electrical wiring. 3. Wiretapping 4. Natural disaster 5. Supply shortage 6. Damage caused by service provider.	Power failure Short circuit and fire Communications services breakdown Cyber Crime / Attack System unavailable

APENDIX-6: Relationship between vulnerabilities and risk frequency rating along with risk Scenarios

SL	Assets	Risk Scenarios	Risk Frequency Evaluation	Vulnerabilities (Yes/No)	Risk frequency Rating
1.	Core Application Software	Software failure	Effectiveness of controls to mitigate well-known flaws and maintain change management in the application is rated a High, hence threat occurrence is rated as low.	No	0.1
		Hardware failure / damages	As proper control is in place for least privilege and maintains change management, hence the Hardware failure / damage occurrence is rated as low.	No	0.1
		Denial of Service (DoS / DDoS)	Session limiting is properly configured at all network security devices, hence DDOS occurrence possibility is low.	No	0.1
		Unauthorized access to information system, Social engineering, Theft	Operating Systems, Security patch and Browser Applications are regularly updated and Internet access from server is tightly restricted, hence likelihood of unauthorized access to information system, social engineering and theft is medium.	Yes	0.5
		Compromising Confidential information	Likelihood of compromising confidential information is low due to Security Awareness Training program employees are well aware.	No	0.5
		Malicious code inject by insider or outsider	Possibility of malicious code inject by insider or outsider is low, because developers are strictly maintaining application security e.g. input validation, SDLC framework etc.	No	0.1
		Disclosure of passwords	Likelihood of disclosure of passwords is low, due to Security Awareness Training program employees are well aware.	No	0.5
		Social engineering	Due to properly incorporating Firewall/IPS/WAF in place, likelihood of social engineering is low.	No	0.1
		Inability or limited ability to perform missions/business functions, Delay of projects.	Operational documentation and procedure and procedure (for user and administrator) are prepared properly for Application / software.	No	0.1
		System unavailable	Chance of unavailability is poor, due to every device in information technology is properly backed up and redundant.	No	0.1
		Disclosure of sensitive information	Proper encryption in proper place is strictly maintained.	No	0.1

SL	Assets	Risk Scenarios	Risk Frequency Evaluation	Vulnerabilities (yes/No)	Risk frequency Rating
2.	End-User Application Software	Software failure	As flaws in the software are properly checked and rectified, hence the thread occurrence is low.	No	0.1
		Cyber Crime / Attack	As applications are updated with latest security patched regularly, possibility of cyber-crime attacks is low.	No	0.1
3.	In-house developed Applications	Software failure	Possibility of software failure is low due to data / input validation in software is strongly maintained.	No	0.5
		Cyber Crime / Attack	As flaws in the software are properly checked and rectified and application security is properly maintained, possibility of cyber-crime attacks is low.	No	0.5
4.	Databases	Database software failure	High availability is maintained	No	0.1
		System failure	Due to high availability for storage and power maintained, the threat occurrence of system failure is low.	No	0.1
		Malicious code inject by insider or outsider	Threat occurrence of malicious code inject by insider or outsider is low, because internet access is restricted by WSA, unwanted ports are closed by Firewall, web application is filtered by WAF, and Data query is programmatic.	No	0.1
		Disclosure of passwords	Likelihood of disclosure of passwords is low, due to proper encryption is placed on database.	No	0.1
		Unauthorized access to information system, Theft	Database Systems Security patch are regularly updated and Internet access from server is tightly restricted, hence likelihood of unauthorized access to information system, and theft is medium.	No	0.1
		System unavailable	Chance of unavailability is poor, due to every device in information technology is properly backed up and redundant.	No	0.1
		Disclosure of sensitive information	Proper encryption in proper place is strictly maintained.	No	0.1
5.	Storages	Power failure	Due to regular maintenance and highly physical protection including redundancy, the threat of power failure is low.	No	0.1
		Disk failure	The likelihood of disk failure is low due to proper installation and proper maintenance of the system.	No	0.1
		Hardware	The likelihood of hardware malfunction is low	No	0.1

		malfunction	due to proper installation, protection of storage, replacement schemes and proper maintenance of the system.		
SL	**Assets**	**Risk Scenarios**	**Risk Frequency Evaluation**	**Vulnerabilities (yes/No)**	**Risk frequency Rating**
		Software failure	The likelihood of software failure is low due to proper installation, replacement schemes, and proper maintenance of the system.	No	0.1
		Unauthorized access to information system	The likelihood of unauthorized access to information system is low due to proper protection, and sufficient maintenance of the system.	No	0.1
		System unavailable	Chance of unavailability is poor, due to every device in information technology is properly backed up and redundant.	No	0.1
		Cyber Crime / attack Malicious code inject by insider or outsider	Possibility of Cyber Crime / attack by insider or outsider is very low due to proper monitoring is fully effective.	No	0.1
		Disclosure of sensitive information	Proper encryption in proper place is strictly maintained.	No	0.1
6.	Information (Data)	Cyber Crime / Attack	Possibility of Cyber Crime / attack by insider or outsider is medium due to authorized software is fully maintained and Security Awareness training IS conducted on regular basis.	No	0.1
		Theft	Possibility of theft by insider or outsider is very low due to proper monitoring is fully effective and all environments are completely separated.	No	0.1
		Hardware/software failure	Due to maintaining high availability on storage and power system, the occurrence of threat on hardware or software failure is low.	No	0.1
		Corruption of data	Due to incorporate proper hashing, encryption, OTP etc. and removing unnecessary program/services, data is secured.	No	0.1
		Communications services breakdown	High availability is properly maintained, hence risk of breakdown of communication service is medium.	No	0.1
		System unavailable	Chance of unavailability is poor, due to every device in information technology is properly backed up and redundant.	No	0.1

SL	Assets	Risk Scenarios	Risk Frequency Evaluation	Vulnerabilities (yes/No)	Risk frequency Rating
7	Network Equipment	Hardware Malfunction /failure	All hardware components are redundant. Also proper monitoring is in place.	No	0.1
		Communication link down	High availability on communication links are highly effective. So the threat of occurrence is medium	No	0.5
		Cyber Crime / Attack	Network Firewall with IPS, WAF, Web Security Appliance, Email Security Appliance are in duly placed, hence possibility of Cyber Crime / Attack is low.	No	0.1
		Power failure	Due to maintaining high availability and proper monitoring the threat occurrence is low.	No	0.1
		Evidence missing / Forensic issue after any occurrence	As NTP is strictly maintained as per policy.	No	0.5
8.	Operating Systems Software	Cyber Crime / Attack	As Operating systems security patch are updated, possibility of cyber-crime/ attacks is low.	Yes	0.5
9.	Hardware Systems	Hardware malfunction/ failure	humidity, dust, soiling, sensitivity to electromagnetic radiation, power system high availability are maintained and monitored proactively, hence chance of hardware malfunction/failure is low.	No	0.5
		Power failure	Redundant power supply, battery and generator backups are accurately maintained and monitor, hence livelihood of power failure is low.	No	0.5
		Unauthorized access to information system	As access control is strictly maintained, possibility of unauthorized access to information system is low.	No	0.1
10.	Datacenter Premises	Flood	Data centers has adequate height of ground floor and well-organized to prevent and redress the flood.	No	0.1
		Fire (Burning)	Height of ground floor of Datacenter has adequate space and all the walls are fire resistant, hence Data center has effective control in place to prevent and redress the fire.	No	0.1
		Earthquakes	Data centers are designed in a way that it can survive from earthquake.	No	0.1
		Long-term power failure	Redundant power supply, battery, UPS and generator backups are accurately maintained and monitored, hence likelihood of long-term power failure is low.	No	0.1
11.	Human Resources (People)	Disgruntled Employee	While recruiting employee background are screening with due diligence and training on Business etiquette regularly conducted.	No	0.1
		Political Spying	has policy which is enforcing regularly for any unethical issues	No	0.1

		human intervention	Any unethical human intervention is strictly Prohibited.	No	0.1
		- Pandemic Flu -Dengue Fever	Has a very healthy environment and also has its own physician.	No	0.1
12.	Datacenter Supporting Equipment	Power failure	Redundant power supply, battery, UPS, generator backups and AVR (Automated Voltage Regulator) are maintained and monitored; hence likelihood of long-term power failure is low.	No	0.1
		Short circuit and fire	Proper electrical wiring has been established to prevent and redress the short circuit and fire.	No	0.1
		Communications services breakdown	Redundancy on IP Telephony and PABX system is present; hence chance of threat is low.	No	0.1
		Cyber Crime / Attack	Due to proper physical security chance of wiretapping is low.	No	0.1
		System unavailable	As physical and electrical wiring security, and others datacenter supporting equipment are secured, the chance of system unavailability is low.	No	0.1

APENDIX-7: Composite Analysis for Risk Assessment

SL	Assets	Risk Scenarios	Probability/ Risk Frequency Rating	Consequences (Impact)	Overall Risk Rating
1.	Core Application Software	Software failure	0.1	100	10
		Hardware failure / damages	0.1	100	10
		Denial of Service (DoS /DDoS)	0.1	100	10
		Unauthorized access to information system, Social engineering, Theft	0.5	100	50
		Compromising confidential information	0.5	100	50
		Malicious code inject y insider or outsider	0.1	100	10
		Disclosure of passwords	0.5	100	50
		Social engineering	0.1	100	10
		Inability or limited ability to perform missions /business functions, Delay of projects.	0.1	50	5
		System unavailable	0.1	100	10
		Disclosure of sensitive information	0.1	100	10
2.	End- User Application Software	Software failure	0.1	10	1
		Cyber Crime/ Attack	0.1	100	10
3.	In-house developed Applications	Software failure	0.5	10	5
		Cyber Crime/ Attack	0.5	50	25
4.	Databases	Database software failure	0.1	100	10
		System failure	0.1	100	10
		Malicious code inject by insider or outsider	0.1	100	10
		Disclosure of passwords	0.1	100	10
		Unauthorized access to information and system, Theft	0.1	100	10
		System unavailable	0.1	100	10
		Disclosure of sensitive information	0.1	100	10
5.	Storages	Power failure	0.1	100	10
		Disk failure	0.1	100	10
		Hardware malfunction	0.1	100	10
		Software failure	0.1	100	10
		Unauthorized access to information system	0.1	100	10
		System unavailable	0.1	100	10
		Cyber Crime/ Attack Malicious code inject by insider or outsider	0.1	100	10
		Disclosure of sensitive	0.1	100	10

		information			
SL	**Assets**	**Risk Scenarios**	**Probability/ Risk Frequency Rating**	**Consequences (Impact)**	**Overall Risk Rating**
6.	Information (Data)	Cyber Crime/ Attack	0.1	100	10
		Theft	0.1	100	10
		Hardware, software failure	0.1	100	10
		Corruption of data	0.1	100	10
		Communications services breakdown	0.1	50	5
		System unavailable	0.1	100	10
		Disclosure of sensitive information	0.1	100	10
7.	Network Equipment's	Hardware malfunction/ failure	0.1	100	10
		Communication link down	0.5	10	5
		Cyber Crime / Attack	0.1	100	10
		Power failure	0.1	100	10
		Evidence missing / Forensic issue after any occurrence	0.5	100	50
8.	Operating System Software's	Cyber Crime / Attack	0.5	10	5
9.	Hardware Systems	Hardware malfunction/failure	0.5	50	25
		Power failure	0.5	50	25
		Unauthorized access to information system	0.1	100	10
10	Datacenter Premises	Flood	0.1	100	10
		Fire (burning)	0.1	100	10
		Earthquakes	0.1	100	10
		Long-term power supply failure	0.1	100	10
11	Human Resources (People)	Disgruntled Employee	0.1	50	5
		Political Spying	0.1	100	10
		Human intervention	0.1	50	5
		- Pandemic Flu - Dengue Fever	0.1	10	1
12	Datacenter Supporting Equipment	Power failure	0.1	100	10
		Fire due to short circuit	0.1	100	10
		Communications services breakdown	0.1	50	5
		Cyber Crime / Attack	0.1	100	10
		System unavailable	0.1	50	5

Rakibul Haque
Senior Principal Officer
ICT & Mobile Banking Department
Bangladesh Krishi Bank
Head Office, Dhaka