-

1. Introduction:

Information Systems (IS) Audit Division of Internal Audit Department (IAD) assesses the IT systems, its management, controls, processes, and operations of the **Foreign Exchange Operation Department (FEOD)** to ensure confidentiality, integrity, and availability aligned with its business objectives. This report comprises the audit observations, associated risks/impacts and recommendations for the period **January – June, 2024**. The audit was conducted on **06-09 January, 2025** and the department has achieved an overall rating of **Marginal (45.92).**

2. Scope:

The IS audit is carried out in accordance by the ICT Security Policy Version 4.0, ICT Risk Management Framework Version 2.0, Backup and Restore Policy Version 1.0, ICT Hardware and Software Usage Policy Version 2.0, and Email Policy Version 2.0 as well as relevant ICT-related administrative circulars, office circulars, and meeting minutes. Additionally, the audit team aimed to cover the following domains:

a) Organization and Management of ICT
b) ICT Risk Management
c) ICT Operation Management
d) Infrastructure Security Management
e) Access Control of Information System
f) Cyber Security Management
g) Acquisition and Development of Information Systems
h) Business Continuity and Disaster Recovery Management
i) Service Provider Management
j) Training and Awareness

3. Current Observations, Risks/Impact and Recommendations:

IS Audit Session: January – June, 2024 (09 observations SL# 01-08)

1) IS Audit report was not responded for two (02) consecutive sessions.

Observation:

The department did not comply the IS audit report recommendations of the last two sessions October 2021–December 2023 and October 2020 – September 2021.

Risk/Impact:

a) Non-compliance of ICT Security Policy Version 4.0, article no 2.2.5.1, “Departments/ Offices shall ensure full compliance of different necessary controls under ICT Security Policy.”
b) IS observations are given to mitigate future risk. If observations are not solved in time it may raise further risks.

Risk Category: High

Recommendation: The department is advised to take necessary steps to comply IS audit report recommendations and send reply to Internal Audit Department in due time.

2) Improper management of old and unused ICT assets

Observation:

During audit old and unused ICT assets are found scattered in various places of the department. This is a sign of asset mismanagement and lack of user awareness.

Risk/Impact:

a) Scattered assets are easy to misuse or modify. Non-compliance of ICT security Policy (V4), article 5.2.9 – "ICT assets shall be adequately protected from unauthorized access, misuse or fraudulent, modification, insertion, deletion, substitution, suppression or disclosure."

b) Asset tracking will be difficult.

c) If any asset is out of order it should be sent to proper authority to claim warranty (if available) as early as possible.

Risk Category: High

Recommendation: The department is advised to:

a) Maintain an asset inventory register with detailed information, including custodian details.

b) Include information on unused, disposed, and in-stock assets in the inventory.

c) Maintain year-wise summary of ICT asset-related information.

3) Incomplete ICT asset documentation and inventory records

Observation:

ICT asset related documents are found without custodian signature. Information of old and Unused assets information are not included in ICT asset inventory. Printer information is also missing in ICT asset inventory.

Risks/Impact:

a) Non-compliance of ICT Security Policy (V4) control number 2.2.6.3 "ICT Security Maintenance Team will Maintain and review ICT asset inventory with custodian details and data classifications to make asset and information security labeling and handling properly**".**

b) Asset tracking will be difficult.

Risk Category: High

Recommendation: The department is advised to keep ICT asset inventory register up-to-date stating with significant details including custodian signature. Unused but functional ICT assets should be stored in a secure room to avoid asset mismanagement.

4) Lack of awareness in data backup process

Observation:

Currently only FTP file server is allowed for keeping user data backup which is managed by ICT department. But most employees are not aware of this process. No backup register is being maintained.

Risk/Impact:

a) In case of hard disk failure, no backup will be available to continue the business process.

b) Non-compliance of ICT Security Policy (V4) control number 9.5.6 – "The backup inventory and log sheet shall be maintained, checked and signed by the supervisor."

c) Non-compliance of the article 9.5.1 ICT Security Policy (V4) – "An approved Backup and Restore Policy shall be in place."

Risk Category: High

Recommendation: The department is advised to-

a) Aware employees to keep backup of official data to avoid data loss in case of computer disk failure.

b) Maintain log sheet according to mentioned ICT security policy.

5) User Lists of Export-Import related software are not up-to-date

Observation:

The department uses 09 (nine) different software related to export and import but provided user list for this software is outdated. Many users are transferred from FEOD but still found in the provided software user list.

Risk/Impact:

a) Unauthorized users with privileges may access, modify, change system information without permission or prior knowledge of authority which may cause system vulnerability.

b) Non-compliance of ICT Security Policy Version 4.0, article number 6.1.8, "Access privileges must be changed/ locked immediately when users' status changes or left the bank."

Risk Category: High

Recommendation: The department is advised to maintain updated user list regarding export and import related software. Furthermore, the department should deactivate transferred employees immediately.

6) Business Continuity Plan (BCP) is incomplete and outdated

Observation:

BCP is outdated. It was last updated on 24/12/2023. BCP contains following lapses:

a) Information about application/software used by the department are not available.

b) Departmental data backup is not updated with current practice.

Risk/Impact:

a) Non-compliance of ICT Security Policy Version 4.0, article number 9.2.4 – "An approved Business Continuity Plan addressing the recovery from disaster to continue its operation shall be in place. This plan should be based on the long-range IT plan and should support and be aligned with the overall business continuity strategy."

b) Non-compliance of ICT Security Policy Version 4.0, article number 9.2.4(b) – "BCP shall address the strategy and well-defined roles and responsibilities."

Risk Category: High

Recommendation: The department is advised to-

a) Include name of all software related information in BCP.

b) Update the data backup section in BCP to reflect the current data backup process (FTP file server), replacing the outdated practice of using CD/DVD.

7) DMS is not being used properly

Observation:

Document Management System (DMS) is not activated properly in the department. During IS audit it is observed that, official documents are not properly distributed among lower level executives and total 10141 documents are still found in pending status.

Risks/Impact:

a) Due to lack of proper use sensitive document is lost or cannot be tracked properly.

b) Non compliance of Office Order HRD-1:24/2013 and Administrative Circular - HRD-1/2013-15

Risk Category: High

Recommendation: The department is advised to follow the mentioned office order regarding Document Management System (DMS).

8) Lack of user awareness observed

Observation:

Following lack of user awareness is observed during IS audit:

a) Password is being saved in browser by few user.

b) Official Email and intranet portal was found open and computer was unlocked while user was not present at the desk.

Risk/Impact:

a) According to HRD Office order **14/2016**, Date: **03 March, 2016** – "কোন অবস্থাতেই *Unattended* অবস্থায় পিসি খোলা রাখা যাবে না এবং অফিস ত্যাগ করার সময়ে অবশ্যই পিসি বন্ধ করতে হবে।"

b) In this scenario password can be leaked and unauthorized access may happen to their email account. This can be a non-repudiation issue. **Non-repudiation** is a key security principle in **Information Systems (IS) Audit** that ensures a person or system **cannot deny** performing an action, such as sending a message, approving a transaction, or accessing a system.

Risk Category: Medium

Recommendation: The department is advised to take necessary steps to aware employees regarding the risk of saving password in browser and follow the mentioned office order accordingly.

4. Compliance Status of Previous Audit:

Foreign Exchange Operation Department has complied only 16 out of 55 recommendations given in the previous audit report and the remaining findings were found in the process of compliance.

SL.	Audit Period	Observations	Compliant	Non-compliant
A)	October 2021–December 2023	11	0	11
B)	October 2020-September 2021	9	0	9
C)	April 2019 - September 2020	6	0	6
D)	October 2018-March 2019	8	3	5
E)	April 2018-September 2018	21	13	8
Total		**55**	**16**	**39**

Remarks

- All non-compliance observations of the previous consecutive audit reports are incorporated in this report.
- The status of compliance reported **'in process but not yet complete'** has also been considered as non-compliance.
- Reference to Risk/Impact is mentioned from **ICT Security Policy Version 4.0**.

5. Observations, Risks/Impact and Recommendations from previous IS audit:

A. IS Audit Period: October 2021–December 2023 (11 Observations Serial #09-19):

9) **Observation:**

Compliance status of last audit report is not found.

Risk/Impact:

a) Non-compliance of the article 2.2.5.1 ICT Security Policy (V4) – "Departments/ Offices shall ensure full compliance of different necessary controls under ICT Security Policy."

b) IS observations are given to mitigate future risk. If observations are not solved in time it may raise further issue.

Risk Category: High

Recommendation: The department is advised to take necessary steps to comply IS audit report recommendations and send reply to Internal Audit Department in due time.

10) **Observation:**

During audit old and unused ICT assets are found stored at department (5th floor).

Risk/Impact:

a) Scattered assets are easy to misuse or modify. Non-compliance of ICT security Policy (V4), article 5.2.9 – "ICT assets shall be adequately protected from unauthorized access, misuse or fraudulent, modification, insertion, deletion, substitution, suppression or disclosure."

b) Asset tracking will be difficult.

c) If any asset is out of order it should be sent to proper authority to claim warranty (if available) as early as possible.

Risk Category: High

Recommendation: The department is advised to send out of order (non-functional) assets to proper authority to claim warranty (if available). Other assets should be store in a secure place with keeping records in departmental ICT asset inventory list.

11) **Observation:**

Approved ICT asset related documents are not found as ready reference. Old and Unused assets information are not included in ICT asset inventory. Printer information is also missing in ICT asset inventory.

Risks/Impact:

a) Non-compliance of ICT Security Policy (V4) control number 2.2.6.3 “ICT Security Maintenance Team will Maintain and review ICT asset inventory with custodian details and data classifications to make asset and information security labeling and handling properly**”.**

b) Asset tracking will be difficult.

Risk Category: High

Recommendation: The office/department is advised to maintain asset inventory register with significant details including custodian details. Unused, disposed and in stock assets information should be a part of asset inventory.

12) <u>**Observation:**</u>

It is mentioned in BCP that - "All (AD & above) will backup their important files" but this practice is not maintained. CD/DVD is mentioned as backup medium, but currently only FTP is allowed for keeping backup which is managed by ICT department.

Risk/Impact:

a) In case of hard disk failure, no backup will be available to continue the business process.

b) Non-compliance of ICT Security Policy (V4) control number 9.5.6 – “The backup inventory and log sheet shall be maintained, checked and signed by the supervisor.”

c) Non-compliance of the article 9.5.1 ICT Security Policy (V4) – “An approved Backup and Restore Policy shall be in place.”

Risk Category: High

Recommendations: The department is advised to-

a) Update data backup section of BCP mentioning current practice of data backup process instead of CD/DVD- which is obsolete now.

b) Aware employees to keep backup of official data to avoid data loss in case of computer disk failure.

c) Maintain log sheet according to mentioned ICT security policy.

13) <u>**Observation:**</u>

Electric circuit board is found blocked by paper box and iron safe which may create hazardous situation.

Risk/Impact:

Blocking electric circuit board with obstacle may arise multiple problem including fire hazard, component damage, difficulty in maintenance etc.

Risk Category: High

Recommendation: The department is advised to maintain cleanliness in the area around the electric circuit board.

14) <u>**Observation:**</u>

The **International Card Monitoring System (ICMS)** software has encountered the following User Interface related issues:

a) Data fails to load when selecting all banks.

b) Problem with selecting date ranges.

c) Software becomes unresponsive and sluggish when loading large datasets.

Risk/Impact:

a) Data loading error disrupts daily operations, affecting the efficiency of FEOD’s day to day operation and potentially delaying critical decision-making.

b) Non-compliance of ICT Security Policy (V4), article number 8.6.4, “Any bugs and/or defects found due to design flaws must be escalated to higher levels of Bangladesh

Bank and/or Software vendor organization in time. ”

Risk Category: Medium

Recommendation: The software system must function seamlessly across all scenarios. For handling large datasets, it's advisable to implement pagination and adopt lazy loading techniques to ensure optimal performance and efficient data retrieval. This approach will enhance usability and prevent system slowdowns associated with loading extensive amounts of data at once.

15) **Observation:**

The **International Card Monitoring System (ICMS)** software has encountered numerical floating point error while calculating total amounts of posted records for “Bank wise invisible payments”.

Risk/Impact:

a) Flawed calculations in software system could lead to financial inaccuracies, incorrect financial reporting, or discrepancies in financial audits.

b) Non-compliance of ICT Security Policy (V4), article number 8.6.4, “Any bugs and/or defects found due to design flaws must be escalated to higher levels of Bangladesh Bank and/or Software vendor organization in time. ”

Risk Category: Medium

Recommendation: Error in software is bad even floating point number is not tolerable. It is recommended to fix floating point value accurately in the software system to improve business value.

16) **Observation:**

BRD (Business Requirement Document) document was not found as ready reference for the following software: International Card Monitoring System, Money Changer Exchange System, Export Monitoring System and Import Monitoring System.

Risk/Impact:

Non-compliance of ICT Security Policy (V4), article number 8.4.3, “Detailed business requirements shall be documented and approved by the competent authority.”

Risk Category: Medium

Recommendation: To get high level understanding of the business process it is important to have BRD document for any new or old software. It is recommended to prepare BRD document for this software consulting with business people and its stockholders. This will provide any new user of the system to have clear understanding of the system business process.

17) **Observation:**

Password is being saved in browser by some user which is happening due to lack of awareness.

Risk/Impact:

Password can be leaked and unauthorized access may happen. It is easy to extract sensitive information from Web browsers for lots of malware. Web browsers are fairly easy to break into, and lots of malware, browser extensions and even honest software can extract sensitive information from them.

Risk Category: Medium

Recommendation: The department is advised to take necessary steps to aware employees regarding the risk of saving password in browser.

18) **Observation:**

Following issues are found with **Money Changer System**:

a) Documentation for user creation is available, but user deactivation document was not found as ready reference.

b) The system has user manual which exist in help menu section, but this menu is not working.

Risk/Impact:

a) Non-compliance of ICT Security Policy (V4), article number 8.4.10, “System documentation and User Manual shall be prepared and preserved by the concerned department(s) as ready reference."

b) Non-compliance of ICT Security Policy (V4), article number 2.5(h), "The followings shall be documented properly: h) User manual of all applications for internal/external users."

Risk Category: Medium

Recommendation: Ensure the Money Changer System has a readily accessible and comprehensive user manual covering all functionalities, including user creation and deactivation procedures. Resolve the issue with the non-functional help menu by making it accessible and functional for all users.

19) **Observation:**

BCP is found updated but team members are not aware of their roles and responsibilities. (For example: Zahidul Haq is one of data backup team members but he is not aware regarding this.)

Risk/Impact:

a) ICT Security policy (V4), article number 9.2.5, "BCP shall be circulated to all relevant stakeholders. The recipients shall receive a copy of amended plan whenever any amendment or alteration takes place."

b) Non-compliance of ICT Security policy (V4), article number 9.2.3, "BCP shall address the strategy and well-defined roles and responsibilities."

Risk Category: Medium

Recommendation: The department is advised to aware BCP members regarding their roles and responsibilities through regular team meetings.

B. ICT Audit Period: October 2020 – September 2021 (9/9 Observations Serial #20-28)

20. **Observation:** (Original report serial number is 01)

Compliance of last audit report is absent.

Risks/Impact:

Non compliance of ICT Security policy Version 3.0, article 2.5.1 & 12.1

Risk Category: High

Recommendation: The department is strongly advised to send compliance status to Internal Audit Department within due date.

21. **Observation:** (Original report serial number is 02)

Asset inventory does not have any approval. Only PC information exists here. Moreover, it does not have others ICT accessories information such as printer, scanner, ups etc. Besides, Asset inventory needed to include custodian signature and PC model number/information.

Risks/Impact:

Non compliance of ICT Security policy Version 3.0, article 2.1.6.3, 5.1.4 & 5.1.6

Risk Category: High

Recommendation: The department is advised to keep the custodian signature and other necessary information (mentioned in the ICT Security Policy) in the ICT asset inventory register for IT equipments.

22. **Observation:** (Original report serial number is 03)
Some PCs are showing "your device is missing important security and quality fixes" message in windows security update. OS versions of these PCs are 1909/20H2 which are quite old and needed to update. (Ref. Host: HOD0215FEOD05A, HOD0820FEOD11, HOD0820FEOD12, HOD1014FEOD15)
Risks/Impact:

a) Deviation from standard configuration.
b) Non compliance of ICT Security policy Version 3.0, article number 5.4.10(b)

Risk Category: Medium
Recommendation: The department is advised to take necessary steps to ensure the security through regular update of the Windows.

23. **Observation:** (Original report serial number is 04)
In case of some PCs, user "Administrator" is active, though it is strictly prohibited. (Ref. Host: HOD0215FEOD05A, HOD0215FEOD81, HOD1014FEOD13, HOD1014FEOD070, HOD215FEODGMQ1, HOD0215FEOD02, HOD1014FEOD14A, etc.)
Risks/Impact:
Non compliance of ICT Security policy Version 3.0, article number 5.2.1 & 6.5.3
Risk Category: High
Recommendation: The department is advised to take necessary steps to prohibit the use of unauthorized user credential (id/password).

24. **Observation:** (Original report serial number is 05)
In case of some PCs, BB standard configuration is found missing. As for example- Standard windows log size is missing, Auto play is found On by default. (Ref. Host: HOD0215FEOD02, HOD0618FEOD01, HOD1014FEOD14A, HOD0820FEOD08, etc.)
Risks/Impact:
Non compliance of ICT Security policy Version 3.0, article number 5.2.1 & 6.5.3
Risk Category: Medium
Recommendation: The department is advised to take necessary action to ensure standard configuration for all the PCs.

25. **Observation:** (Original report serial number is 06)
In case of some PCs, removable storage access port is found enable though it is strictly prohibited. (Ref. Host: HODA105FEODBUF8)
Risks/Impact:

a) Non compliance of ICT Security policy Version 3.0, article number 5.2.8
b) Virus, malware or worm may spread through USB port.

Risk Category: High
Recommendation: The department is advised to take necessary steps to ensure the USB port security through disabling when it is not appropriately authorized to keep it open.

26. **Observation:** (Original report serial number is 07)
In case of some PCs, few share folders are observed (D:\New Folder, D:\Sharing is caring, C:\Users etc) though it is prohibited. (Ref. Host: HOD0820FEOD11, HOD0820FEOD12, HOD0820FEOD08, etc.)
Risks/Impact:
Non compliance of ICT Security policy Version 3.0, article number 5.4.10 (e)
Risk Category: High
Recommendation: The department is advised to take necessary steps regarding the share folders to strengthen the security and confidentiality issues.

27. **Observation:** (Original report serial number is 08)
In case of some PCs, Tor browsers (unauthorized VPN software) are observed (location D:\D drive backup, D:\Users\suraia\Downloads, E:\FEOD Important docs Backup\ desktop\ Tor Browser etc) though it is strictly prohibited to use.
(Ref. Host: HOD1014FEOD17, HOD105FEODBUF9, HOD1014FEOD14A, etc.)
Risks/Impact:

Non compliance of ICT Security policy Version 3.0, article number 5.1.15
Risk Category: High
Recommendation: The department is advised to take necessary steps to remove unauthorized software from the PCs.

28. **Observation:** (Original report serial number is 09)
In some cases, few computers are placed in floor level.
Risks/Impact:
Non compliance of ICT Security policy Version 3.0, article number 5.2.16
Risk Category: Low
Recommendation: The department is advised to take necessary action so that all the PCs are placed above floor level.

C. ICT Audit Period April 2019 – September 2020 (6/6 Observations Serial#: 29-34):

29. **Observation:** (Original report serial number is 01)
Formal approval document for creating departmental User ID of the following systems/software is not found:

a) Online Import Monitoring System (OIMS)
b) Online Export Monitoring System (OEMS)
c) Online Inward Remittance Monitoring System (OIRMS)
d) International Card Monitoring System (ICMS)
e) Online TM Form Monitoring System (OTMFMS).

Risks/Impact:
According to ICT Security Policy (January 2018) control number 6.1 "User ID Maintenance form with access privileges shall be duly approved by the appropriate authority" and "Access privileges must be changed/locked immediately when users' status changes or left the bank." Unauthorized users with privileges may access, modify, change system information without permission or prior knowledge of authority which may cause system vulnerability."
Risk Category: High
Recommendation: The Department is advised to maintain approval documents for each system/software users with user creation and deletion/deactivation information.

30. **Observation:** (Original report serial number is 02)
User Acceptance Test (UAT) documents are not found for those software/systems that the department is using (mentioned in observations # 01).
Risks/Impact:
Non-compliance of ICT Security Policy Version 3.0, article number 4.1.6. "User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment. **User Acceptance Testing**, better known as **UAT** is the last section of the whole **testing process** of any software. This process assesses if the system can support day-to-day business and user scenarios and ensure the system is sufficient and correct for business usage and thus increase efficiency of the software over time."
Risk Category: Medium
Recommendation: The department is advised to complete User Acceptance Test for all the software they are using with the help of concern department.

31. **Observation:** (Original report serial number is 03)
No data retention period defined for those software/systems systems that the department is using (mentioned in observations # 01).
Risks/Impact:
Non-compliance of ICT Security Policy Version 3.0, article number 9.3.4, "The details of the planned backup schedule for each business application shall include the retention period for backed-up or archived information and the retention period shall be consistent with business requirements". Proper data backup/preservation will not be ensured without defining data retention period."
Risk Category: High
Recommendation: The department is advised to define data retention period for all systems/applications used.

32. **Observation:** (Original report serial number is 04)

Last ICT audit report compliance was not found as ready reference.

Risks/Impact:

Non-compliance of ICT Security Policy Version 3.0, article number 2.1.5.1, "Departments/Offices ensure full compliance of different necessary controls under ICT Security Policy". Compliance report reflects the actual scenario after the risk based audit was conducted."

Risk Category: High

Recommendation: The department is recommended to send the ICT audit report compliance in time.

33. **Observation:** (Original report serial number is 05)

Backups have been preserved into a shared folder with public access with no encryption or password protection which may lead to sensitive/confidential data leakage/loss.

Risks/Impact:

Non-compliance of ICT Security Policy Version 3.0, article number 9.3, "In case of hard disk failure, no backup will be available. Moreover, public access to backup without encryption or password protection may cause serious problem if it is copied or transferred over internet by anonymous person."

Risk Category: High

Recommendation: The Department is advised to take data backup periodically according to the applicable control/sub control in 9.3 of ICT Security Policy (January 2018). Backup should be preserved on backup media with password protection.

34. **Observation:** (Original report serial number is 06)

During audit time, the audit team found following irregularities in some PCs (Details in attachment):

a) Revocable models are found which are extremely slow to operate
b) Screen saver is found disabled, User should be aware of the risk
c) Remote login service/assistance is found enabled
d) Restore point is not set properly
e) Log file size is found less than the recommended size.
f) Both latest Trend Micro and Previous McAfee anti-virus are running.
g) Only McAfee anti-virus running which is obsolete now
h) Windows is missing important update
i) Windows not activated
j) Some unauthorized software are found (e.g. C/A agent, VLC)
k) Some unauthorized local users like 'admin', 'user' etc is found.

Risks/Impact:

Maintaining PC standardization guideline of Bangladesh Bank is Important for ICT systems best practices and secure use. Without proper standardization security breach might be created to the entire Bangladesh Bank network.

Risk Category: High

Recommendation: The department is advised to take necessary steps to resolve those irregularities with the help of concern department.

D. ICT Audit Period October 2018 – March 2019 (5/8 Observations Serial#: 35-39):

35. **Observation:** (Original serial # 04)

List of software/applications used with user access privilege is not maintained.

Risks/Impact:

Unauthorized users with privileges may access, modify, change system information without permission or prior knowledge of authority which may cause system vulnerability. Department should maintain approved software list used by them which will help to monitor user list, data backup periodically etc.

Risk Category: Medium

Recommendation: The department is recommended to maintain approved list of used software with user access privileges details.

36. **Observation:** (Original serial # 06)

Data backup is not taken as per Backup and Restore Policy.

Risks/Impact:

In case of hard disk failure, no backup will be available. Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss. This is also a part of Disaster Recovery Plan (DRP).
Risk Category: High
Recommendation: The Department is advised to take data backup periodically according to the applicable control/sub control in 9.3 of ICT Security Policy (January 2018).

37. **Observation:** (Original serial # 02)
Updated and approved Business Continuity Plan (BCP) is not found in the department.
Risks/Impact:
It is important for ensuring the applicability of BCP. Unapproved BCP may not effective as well as BCP team members may not be aware of their duties.
Risk Category: High
Recommendation: The department is advised to review BCP according to the applicable control/sub control in chapter 9 of ICT Security Policy (January 2018).

38. **Observation:** (Original serial # 05)
ICT asset inventory is not updated.
Risks/Impact:
It does not ensure proper use of assets and Asset tracking will be difficult.
Risk Category: High
Recommendation: The department is advised to maintain asset inventory register with custodian details according to the applicable control/sub control in 5.1 of ICT Security Policy (January 2018).

39. **Observation:** (Original serial # 08)
There are some users who are running their PC without UPS or Malfunctioning UPS. According to ICT Security Policy (January 2018) control number 5.2.2 "Desktop computers shall be connected to UPS" but some PCs are running without UPS.
Risks/Impact:
When an unexpected power failure occurs, the computer shut down improperly. As a result file corruption, OS corruption or hard disk fatal error may occur.
Risk Category: High
Recommendation: The Department is advised to take necessary action so that all desktop PCs are connected with functional UPS

E. ICT Audit Period April 2018-September 2018 (8/21 Observations Serial#: 40-47):

40. **Observation:** (Original serial # *02*)
Business Continuity Plan (BCP) is not found.
Risks/Impact:
Violation of BB ICT Security Policy. BCP is required for planning of business resiliency for critical incidents.
Recommendation: The department is recommended to place an approved Business Continuity Plan (BCP).

41. **Observation:** (Original serial # *03*)
ICT asset inventory is not maintained properly.
Risks/Impact:
Violation of BB ICT Security Policy. Without asset inventory, department may face problem to manipulate actual assets.
Recommendation: The department is advised to maintain ICT asset inventory properly.

42. **Observation:** (Original serial # *04*)
Data backup is not taken as per Backup and Restore Policy.
Risks/Impact:
Violation of Backup and Restore Policy. Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss. This is also a part of Disaster Recovery Plan (DRP).
Recommendation: The department is recommended to take Data Backup as per policy.

43. **Observation:** (Original serial # *05*)
Some unauthorized software (Tor browser, HP Compaq download manager, etc.) are found in some PCs.

Risks/Impact:

Unauthorized and pirated software may contain viruses, malwares, adware etc. that will damage hard drive, steal sensitive data or cripple the network.

Recommendation: The department is advised to prohibit the employees to install/use all kinds of unauthorized and pirated software.

44. **Observation:** (Original serial # *06*)
Some PCs are running without UPS.

Risks/Impact:

Running computers without UPS may cause damage of hardware and also loss of data.

Recommendation: The department is advised to ensure that all computers are connected through UPS to prevent hardware damage & data loss.

45. **Observation:** (Original serial # *07*)
No action has been taken for disposal of ICT hardware as per policy.

Risks/Impact:

The disposal of assets involves eliminating assets from the accounting records. This is required to completely remove all traces of an asset from asset management register.

Recommendation: The department is advised to take the disposal of ICT hardware as per policy.

46. **Observation:** (Original serial # *08*)
ICT Security maintenance team is not reviewed and updated.

Risks/Impact:

All departmental ICT functions and system may be at risk if the team is not updated.

Recommendation: The department is recommended to review and update the ICT security maintenance team.

47. **Observation:** (Original serial # *09*)
Unused CPU is found open in scattered way.

Risks/Impact:

CPU can be damaged or lost.

Recommendations: The department is advised to take immediate action regarding unused CPU.

6. Domain wise and overall status based on audit observation:

SL.	Security Domains	Status	
		Domainwise	**Overall**
1.	Organization and Management of ICT	Fair	**Marginal** (As per attached sheet)
2.	ICT Risk Management	Marginal	
3.	ICT Operation Management	Fair	
4.	Infrastructure Security Management	Fair	
5.	Access Control of Information System	Fair	

6.	Cyber Security Management	NA	
7.	Acquisition and Development of Information Systems	Marginal	
8.	Business Continuity and Disaster Recovery Management	Marginal	
9.	Service Provider Management	NA	
10.	Training & Awareness	Fair	
11.	Compliance of Last Audit Recommendation	Unsatisfactory	

7. Conclusion:

The department is advised to focus on the security domains that stay in **Marginal** (as described in 6). The department should submit the compliance report to Internal Audit Department, Bangladesh Bank, Head Office, Dhaka by ....

In fine we would like to thank the staff and management of **Foreign Exchange Operation Department (FEOD)** for their co-operation during the course of the review.

Md. Ziauddin Tanvir
Deputy Director (ICT)
Member

Sharifur Rahaman
Deputy Director (ICT)
Member

Md. Jahirul Islam
Joint Director (ICT)
Member

Mitra Sujan
Joint Director (ICT)
Team Leader

Counter Signature

Md. Al-Mehedi Hasan
Additional Director (ICT)

Mamunur Rahman
Director (IAD)