CENTRAL BANK OF THE GAMBIA

CHEQUE IMAGING SYSTEM
(ACP/ACH)

OPERATING RULES FOR PARTICIPANTS

OPERATIONAL RULES FOR THE CHEQUE IMAGING SYSTEM

TABLE OF CONTENTS:

LIST OF ABBREVIATIONS

Abbreviation	Description
ACH	Automated Clearing House
ACP	Automated Cheque Processing
ADT	Automatic Data Treatment: module which enables automatic processing of image files and Data files received from the core banking system or the bank's branches.
ATM	Automated Teller Machine
CBS/CBA	Core Banking System/Core Banking Application
BBAN	Basic Bank Account Number
CAT	Catalogue or Index file describing the package file containing the images.
CBG	Central Bank of The Gambia
CIS	Cheque Imaging System
DATA	Data file generated by the scanning application.
DP	Direct Participant
ENV	Outgoing remittance addressed to the clearing house.
IP	Indirect Participant
ISO	International Standards Organisation
MICR	Magnetic Ink Character Recognition
PAK	Package file, including digital images concatenated.
PKI	Private Key Encryption
POS	Point of Sale
RTGS	Real Time Gross Settlement System
SP	Sub-Participant
WAN/MAN	Wide Area Network/Metropolitan Area Network

OPERATIONAL RULES FOR THE
CHEQUE IMAGING SYSTEM (CIS)

1 RULE 1 GENERAL PROVISIONS

1.1 General

The Central Bank of The Gambia in accordance with its supervisory and regulatory mandate under the Central Bank of The Gambia Act 2005, hereby prescribes the following rules in consultation with relevant stakeholders, for the effective operation of the ACP/ACH system. (See Glossary of Terms - Appendix 1).

The Automated Cheque Processing system (ACP) and the Automated Clearing House (ACH) are to handle large volume and low value payment transactions. The applicable software (**Barberousse-Capture)** enables the scanning of payment instruments (cheques, drafts, bills of exchange, etc). It is to be installed at bank branches or at the Head Offices, in support of the following functionalities:

- Scanning of both sides of payment instruments' (front and back).
- Reading MICR codeline, printing and endorsing text on the reverse side of the scanned instrument;
- Manual input / loading of data related to scanned values
- Generating image files of both sides of the instruments (PAK file) and index files containing information related to the image (CAT file);
- Electronically signing of the images.
- Generating data files containing information of the scanned values;

1.2 Cheque Imaging System

When a customer deposits a cheque at a Presenting Bank, the bank staff will process and submit the cheque information to the ACP through the imaging system.

A cheque scanner is used for capturing images of the cheques (front and back). Banks will also encode additional data on the MICR line (e.g. branch) which will also be captured simultaneously.

The Cheque Imaging System (**CIS)** is a state-of-the-art electronic platform for presenting cheques as "Presenting Banks" to the 'Issuing Bank' for payment. The Issuing Bank processes the cheques for payment in accordance with laid down procedure and communicates the results to the Presenting Bank. **(See Section 17.2)**

1.3 Objective

The CIS system is intended to contribute to the efficient operation of the financial system in The Gambia. The system is expected to increase security of payment processing,

reduce associated risks, and to promote efficiency in terms of speed, cost and robustness.

1.4 Membership

Membership of the CIS shall be mandatory on all commercial banks operating in The Gambia, or any other specialized financial institution as directed by the Central Bank of The Gambia. Membership may also be extended to other institutions, such as Finance Companies, Discount Houses as per the procedures laid out in Rule 2.2 below, and depending on the type of Participant as per Rule 2.1.

1.5 Ownership and Licensing

The CIS system is operated by the Central Bank of The Gambia, which authorises Participants to use the CIS System strictly in accordance with the terms and conditions of the Membership (Participant) Agreement and these Operating Rules. The Central Bank is empowered to regulate the operations and usage of the CIS as it deems fit, or in consultation with members on specific issues from time to time.

1.6 Operating Rules

These rules shall govern the operations and use of the CIS as well as the roles and responsibilities of all Participants, including the Central Bank of The Gambia.

1.7 Amendments to the Operating Rules

These operating rules can be amended when deemed necessary by the Central Bank, in consultation with relevant stakeholders. The Central Bank shall be responsible for implementing the amendments thereof.

1.8 Usage of CIS

1.8.1 Compliance

The Central Bank and all other Participants are bound by the provisions of these Operating Rules. Non-compliance shall be sanctioned via appropriate Regulatory Guidelines as may be issued by the CBG.

1.8.2 CIS Utility

Without prejudice to any laws of The Gambia, all Participants shall use CIS for effecting clearing of inter-bank cheque payments. The CIS system is designed with a back-up system to withstand different scenarios of operational failure (e.g. equipment malfunction etc), thus ensuring business continuity. Participants should refer to Rule 21 for the

relevant procedure to follow under each scenario of hardware, software or network failure.

1.8.3 Current Inter-bank Agreements

Previous Inter-bank agreements relating to Payments, such as the manual Clearing House Rules / Procedures, Inter-Bank Market practices etc, shall cease to exist as and abolished. However, other relevant procedures shall remain in force, except to the extent that they are in conflict with these Operating Rules.

1.8.4 Suspension of Procedures

In the event of unforeseeable circumstances beyond control, either due to potential or real risks:
- (a) The Central Bank may suspend the provisions of these Operating Rules wholly or partially, subject to approval by the majority of Participants and under circumstances where continued operation would undermine the stability of the system.
- (b) During any suspension period, the Central Bank and other Participants must attempt to continue operations as much as possible and in accordance with these Operating Rules.

1.8.5 Participant Consultation

The Central Bank may consult with, and take into account the views of Participants:
- (a) on matters relating to the Terms and Conditions of these Operational Rules; and
- (b) consult through the Bankers Association or its representatives on any issues of significance to CIS operations.

1.8.6 Confidentiality

(a) The Central Bank and all other Participants shall apply the normal rules of banker's confidentiality in all CIS operations. Such confidentiality shall apply in the case of transactions involving individuals, corporations and any other category of customers.

(b) Each party shall instruct its employees, consultants, agents or any other representatives, including its auditors, who will have access to confidential information to maintain such confidentiality as is consistent with these Terms and Conditions. Each party shall treat matters concerning other Participants as if it were its own confidential information.

(c) The provisions of this clause 1.8.6 shall apply even after closure or suspension of the Participant or sub-participant's Account.

2. RULE 2 - PARTICIPANT ACCESS

2.1 Participant Types

CIS supports the following types of participation:

2.1.1 Direct Participant

Direct Participant (DP) is a Commercial Bank which is connected to the Clearing House through its own platform and which is responsible of financial obligations towards other Participants, through its settlement account held at the Central Bank. The DP is a cheque issuing institution and also collects payments from cheques deposited by their customers from other participants on their behalf. The DP must maintain a settlement account with the Central Bank for inter-bank settlement, which must be liquid enough at all times for this purpose.

2.1.2 Indirect Participant

Indirect Participant (IP) is a participant which uses a designated direct participant's settlement account for settlement of net clearing balances. Although known to the Clearing House, IP hold payment accounts but uses direct participating institutions' technical infrastructures for their exchanges with the Clearing House. They are financially liable for all exchanges and their settlement.

The IP receives cheques as Presenting Bank from their customers, but cannot receive cheques as an Issuing Bank, as it lacks the status to issue such instruments to customers. The IP has a direct communication link with the CIS for outward clearing function.

2.1.3 Sub-Participant

Sub-Participant (SP) is a participant without settlement account with the Central Bank and without communication link to the CIS. A Sub-Participant takes part in clearing through a direct or indirect participating institution. In this case, the representative institution (DP or IP) shall assume the financial commitments of the sub-participating institution through its own settlement account. Usually SPs are customers of a DP, with a high volume of cheques for presentation through the DP.

SPs shall be required to establish contractual agreement (Sub-Participant Agreement) with a DP, together with a settlement account. The agreement should determine that the

DP agrees to act as a settlement agent on behalf of the SP. The agreement should also provide legal authority for CBG to debit or credit the DP's settlement account in accordance with the SP's cheque clearing position in the CIS.

The Central Bank shall determine the types of Participants allowed to utilise the CIS from time to time, and may occasionally exclude intending Participants, with reasons.

2.2 Participants Membership

2.2.1 Initial Members

The Central Bank, all licensed commercial banks and other qualified institutions shall be among the initial Participants in the CIS. The list of these participants is as indicated in Appendix II.

2.2.2 Admission of New Members

The Central Bank may authorise the admission of new participants into the CIS, subject to meeting the minimum criteria and execution of the relevant membership agreement(s).

2.2.3 Prerequisites for the Participants

All direct and indirect/sub-participants shall have relevant systems, procedures and competent staff, and shall meet any other criteria which may be determined by the Central Bank from time to time for participation in the CIS. The Central Bank shall continuously monitor Participants to ensure compliance with the specified criteria. Participants shall permit access to their operations and facilities to the Central Bank staff or its representatives for the purpose of such monitoring.

2.2.4 Participant Branch Registration

All bank branches shall be registered for use of the CIS as per Rule 3.4 of these Operational Rules.

2.2.5 Suspension/Expulsion

The Central Bank shall have the sole discretion to suspend or expel a Participant temporarily or permanently if it deems that the Participant has ceased to meet the qualifying criteria prescribed by it from time to time, or if the Participant is declared insolvent or its banking license is revoked by the Central Bank, or the Participant has breached any of the provisions of these Operational Rules, or any other reason deemed appropriate by the Central Bank.

2.2.6 Participants' Withdrawal

A Participant may decide to withdraw from the CIS by giving a formal written 30 days notice to the Central Bank. Upon consenting to the request, the Central Bank shall grant its approval and direct the concerned Participant to surrender its rights, systems, software and any other material that relates to CIS. The Participant is thereafter obliged to comply with the decision.

2.2.7 Revocation of Suspension

The Central Bank may in its sole discretion decide to reverse any suspension (temporal or permanent), of a Participant and notify all concerned parties.

3. RULE 3 – PARTICIPANT CONNECTIVITY

3.1 CIS System Architecture

The CIS operates on **Barberousse-Capture** system architecture for providing its services to the participants. All the application systems and database components of all participants are centrally installed in the CIS data centres (located at the main site and backup site) of the CBG. The **Barberousse-Capture** system is fully web-enabled. Participants are required to access the system via web browser, for performing CIS functions and accessing information of their own CIS databases.

All direct and indirect/sub participants shall set up and maintain a participant platform which comprises PC workstations, cheque scanners and printers for connecting to the **Hannibal ADT** server. The participant platform, connectivity and network requirements are as specified below:

3.2 PARTICIPANT WORKSTATIONS, SCANNER AND PRINTERS FOR CIS

The Participant shall install the following equipment at their premises for performing CIS functions:

3.2.1 CIS Workstations

The head office participants' platform is to be provided by the Central Bank and composes one server and one workstation as follows:

Figure 1: Participant workstation

Participant IT Equipements
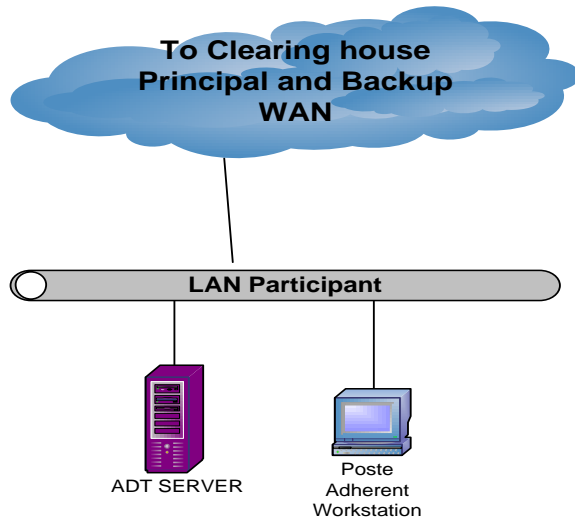
Participants' platforms are configured as follows:

Configuration of ADT Server

The ADT and Oracle is the IBM x3200 M3 server:
- 1 x processor Xeon X3320 2,66 GHz Quad Core.
- 4 Gb of RAM
- 4 SAS disks of 146 Gb in RAID 5
- 2 Ethernet controllers
- 17" Lenovo flat screen L174
- Windows 2008 server standard
- ORACLE Standard Edition.
- ***BFI Software : Hannibal-ADT, Hannibal-ADTAdmin, Hannibal-Autocollecte et Barberousse Générateur des clés***

Configuration of participants workstations

The participant workstation is the Lenovo Think Centre A58 SFF:
- Intel Pentium Dual-Core processor 2.60GHz
- 2 GB RAM
- Disk of 360GB with two partitions
- LENOVO Thikvision L197 wide 19"
- DVD Writer
- Windows XP Pro
- ***BFI Software : Hannibal Poste Adhérent***

Equipments to be acquired by Participants

Acquisition of branch equipments shall be the responsibility of Participants, including Workstations and scanners that will be used by branches of individual banks. However, propriety licenses for branch software shall be provided to all Participants.

BFI Software: **Barberousse-Capture**, **Barberousse - GenerateurCles, Braberousse-GIP.**

Branch workstations

The minimal recommended configuration of the **Branch** workstation is:
- Processor Intel Dual Core 2,0 GHz
- Memory : 1GB RAM
- 80GB Hard drive
- Ethernet card 10/100 Mb
- USB 2.0 (connection needed for LS100 Reader)
- DVD writer
- 17" screen
- Windows XP professional

3.2.2 CIS CHEQUE SCANNER

The CIS cheque scanner must meet the following specifications:
The proposed scanner is the CTS-LS100.
The LS100 scanner is a CTS brand model which provides all necessary scanning functionalities. The main features of this scanner are:
- Speed: 60 doc/minute
- Automatic feeder (100 documents)
- 1 output feeder
- Recto/verso camera
- MICR CMC7 and E13B reader
- OCR recognition
- Ink jet printer
- Image resolution : 100 and 200 dpi
- Grey level : 16, 256 and RGB Color
- Images format : DIB, BMP, JPEG et TIFF
- USB 2.0 connexion (USB1.1 compatible)

3.2.3 CIS PRINTERS

The participant must acquire Ink Jet Printers or compatible alternatives that will function within the CIS framework as per Section 3.2.2 of these Operational Rules.

3.3 Participant Head Office Connectivity

Each participant shall establish a communication link between their head offices and the Central Bank systems. The **Barberousse-Capture** system shall be used as the communication network to provide the link between Participants. It provides primary communication links and backup communication links to the CBG main data centre and backup data centre respectively. The participants shall connect their CIS platform, which comprise workstations, scanners and printers, via communication links to CIS **Barberousse-Capture** system.

3.4 Participant's CIS Branch Connectivity

Each participant must connect all their bank branches to the CIS system. The participant shall be responsible for establishing the network connections between their head office and branches for accessing CIS functions. To do so, the participant must be responsible for performing the following:
- Inform CBG of the location of branches, number and name of users accessing CIS;
- Set up the participant internal network between the branch and head office;
- Inform the Banking Department at the CBG of any new branch openings.

CBG shall maintain the branch codes and other relevant information in their database.

3.5 Communication Bandwidth

The participant shall ensure that there is sufficient communication bandwidth allocated to the CIS communication links at their head office and their CIS branches.

It is required that the communication network bears the following features:

- Uses a switch that supports VLAN dedicated to the participant platform.
- Has at minimum 100 Mb LAN between local machines.
- Connects the participant platform to the network of the clearing house.
  Connects the server of **Hannibal-ADT** to the participant's internal network (linking the head office to the branches).

4. RULE 4 - SYSTEM OPERATIONS

4.1 Role of CBG

CBG shall conduct the daily operations of the central CIS Hannibal ADT system. The daily operations of the central system provide the following business processes:

• Receives cheques from Presenting Bank for outward clearing
• Dispatch cheques to respective Issuing Bank for inward clearing
• Receives replied cheques and returned/rejected cheques from Issuing Bank
• Dispatch replied cheques and returned/rejected cheques to Presenting Bank
• Generate the net settlement for all outward/inward and retuned/rejected cheques and complete settlement in RTGS through DPs' settlement accounts
• Perform end of session settlement for each session of the current business day
• Start CIS session for the next business day.

The CBG shall have the authority for systems administration, security, parameters as well as bank and user administration.

4.2 Clearing Sessions

Cheques are cleared within individual clearing sessions during CIS daily operations.
Each CIS clearing session shall be defined with the following parameters:
• **Clearing Date** – the business day on which cheque clearing shall be completed.
• **Currency** defines the cheques of specified currency (Dalasi), which will be cleared within the clearing session.
• **Session Start** – the time within a business day when the session starts
• **Session End –** the time within a business day when the session ends

4.2.1 Regular Clearing Session

This session configuration will handle regular clearing items. It shall have the following settings for a particular clearing day:

• **Starts** at 14:45 pm previous business day,

• **Cut-off** (end of presentation) will be at 13:30 pm on the clearing day (cheques

presented after that time will be assigned the session date of the next day).

CBG reserves the right to adjust the actual start time/end time of each session on any

business day. Under such situation, CBG shall advise all participants in advance via

system notification or broadcast messages.

4.3 Cheque Clearing Cycle

The Automated Clearing House (ACH) system is established for the processing of electronic inter-bank payments, including cheques valued at not more than the threshold as set by CBG. Examples of inter-bank payments also include salary and pension payments, regular remittances by individuals, and direct credits and debits.

There will be two main types of payment order:

- **Direct debits**, such as utility company payments, but also including the clearing of cheques, where the payment order flows from the Presenting Bank to the issuing bank and the funds flow in the reverse direction (from the issuing bank to the Presenting Bank).
- **Direct credits**, such as salary payments, where the payment order and the funds flow in the same direction from the Presenting Bank to the receiving bank.

Generally, non image values include:

- Direct Credits

- Direct debits;

- Card transactions.

Participants shall ensure that their CIS systems are fully interfaced with their core banking applications to prevent any forms of manual interventions. Failure to do so shall be punishable as may be determined by the CBG from time to time, **unless where approval is granted by CBG to operate without otherwise.**

4.4 CIS Business Calendar

The CIS Business Calendar shall be the business/working days of the Bank. The Central Bank shall also update the calendar through the system or other forms of communication in the event of any unscheduled (**'sudden'**) public holidays. Central Bank shall endeavour to update the system calendar prior to the commencement of the 'sudden' holiday(s). All government working days shall be the CIS working days, unless the Central Bank issues a circular to the contrary. The date format in CIS shall follow the Gregorian calendar.

4.5 Normal Business Hours Timetable

The business operating hours of CIS, on every normal business day of every week which starts from Monday to Friday, are as indicated in the following diagram and the rest of Sub-section 4.5.

Figure 2: Clearing Schedule
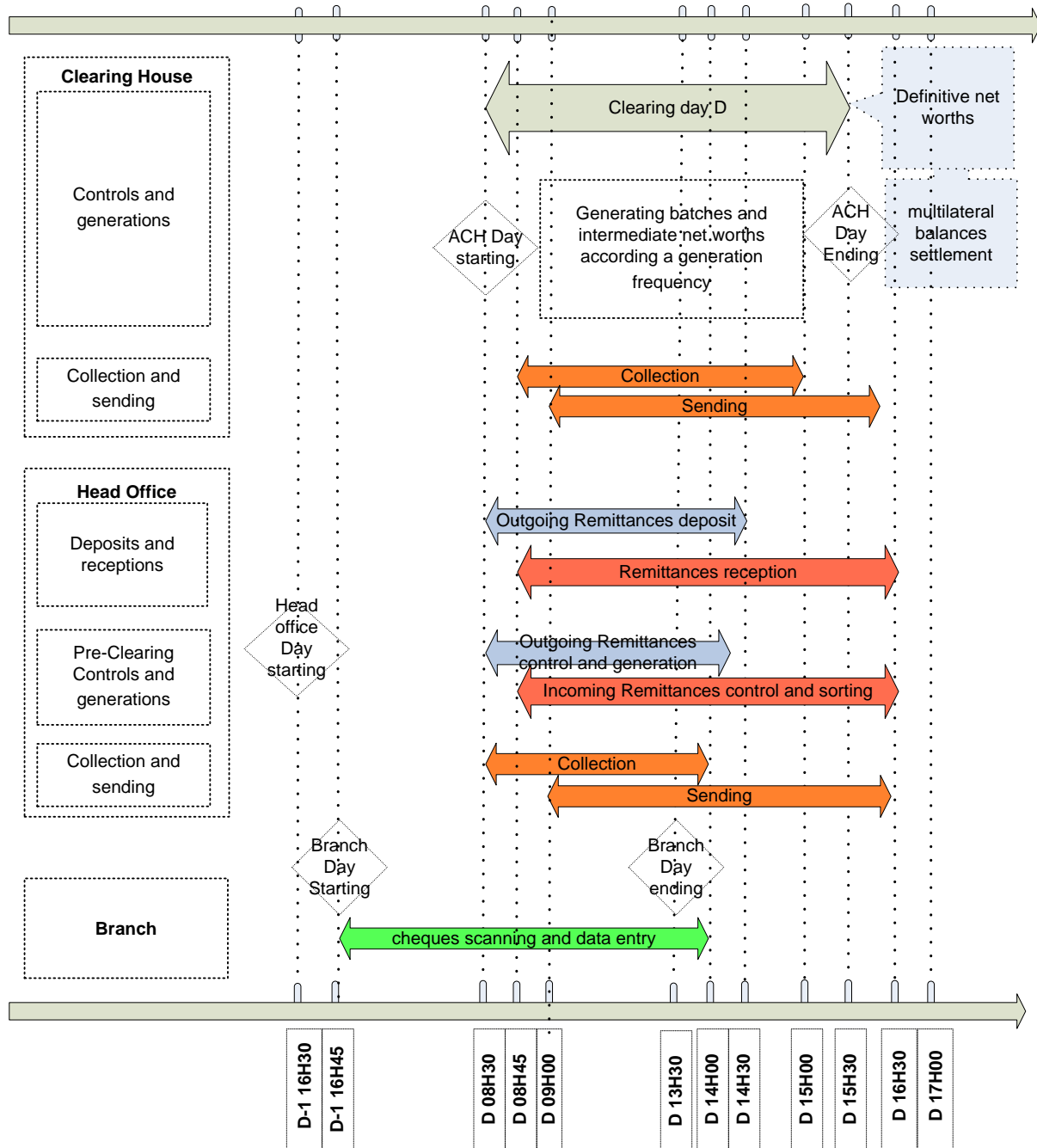
Where:

D-1	**= start of business from the day before the clearing date**
D	**= the clearing day in question**
D+1	**= the following day after the end of business of the clearing day**

At the branch level:

As soon as the branch receives the new "date" file (16h30 of D-1 maximum), it can commence a new day (D). All transactions processed will be kept in the branch Mailbox and collected by the head office at the collection commencement time (08H30 of D). Transactions to be sent to clearing can be processed in the branch until shortly before the head office collection ending time (14H00 of D).

The branch will start receiving inter-bank and intra-bank remittances from the head office at (09H00 of D), till the HO sending termination time of (16H30 of D).

At the head office level:

- Collection of files**:** During the HO collection period (08:30 to 14:00 of D), the head office will collect all files created at branch level in order to control them and integrate them in the remittances to be sent for clearing. Files coming from the CBS/CBA will also be processed during the same period.

Last remittances will be generated by the head office at the end of the generation period (14:15).

Remittances deposit for clearing can be done during the deposit period (08:30 to 14:30 of D): Each deposited remittance will be controlled, encrypted, compressed and placed in the Out mailbox of the head office.

- Reception of files: the head office will start receiving Files from the clearing house as the ACH starts sending them at (09:00 of D), till the end at (16:00 of D). These files are controlled and sorted by HO and then sent to branches for payment (or rejection)

- Sending of files: the sending of files to branches can be done during the HO collection period (09:00 to 16:30 of D).

At clearing house Level: controlling batches, processing and sorting by recipient Participant:

- Collection of files: During the ACH collection period (08:30 to 14:00 of D), the Clearing house will collect outgoing remittances created at head Office level in order to control them and integrate them in the clearing process. Rejected files are sent back to the remitting Participant.

- Generation of return remittances: during the generation period (08:30 to 15:00 of D), the clearing House will continuously send return remittances and intermediate net balance to the recipient Participants.

At the End of the Clearing day (15:30 of D): the clearing house generates files to all Participants as follows:

- Final net balances containing presented, cancelled, and rejected instruments during the clearing day.
- Processing reports,
- Last Return remittances.

Sending of return files to Participants will continue until the end of sending time (16:00)

Final net balances of different participating institutions are communicated to the RTGS system for settlement.

The Central Bank reserves the right to alter the commencement and termination times of each business period, depending on the operating environment. The Central Bank shall communicate by a circular, broadcast or equivalent communication mechanism if there is a change in the business hours of a specific day.

4.6 End of Session Cheque Reply

4.6.1 Cheques not replied at end of day

The CIS shall adopt the 'auto-accept' configuration for regular urgency cheques not replied by Issuing Banks at the end of regular clearing session (also called 'time out cheques'). In 'auto-accept' configuration, all non-replied cheques will be treated as confirmed to be paid by Issuing Banks. All participants are required to make their best effort to process inward cheques and reply them within the same clearing session, in order to complete a same day (D) clearing cycle.

4.7 System Parameters

CBG shall define the following system parameters to be adopted in the daily operations:
- **Max Cheque Amount**:- the maximum cheque amount that can be sent through the system as any cheque exceeding that amount must be presented in a special clearing session *(to be determined by CBG from time to time).*
- **Maximum Cheque Age**: maximum age for a cheque to be considered stale. The usual period is 6 months.
- **Maximum re-presentation cycle -** cheques may be re-presented up to three times, including the initial presentation. Cheques can be re-presented within the same clearing session. The three time presentation shall apply on all clearing cheques, either the same or at consecutive/non consecutive clearing sessions, at day D or D+1**.**
  o **Maximum Batch Cheques Count**: limits the number of cheques captured per batch to, e.g 99 cheques.
  o **Debit cap limit**:- a bank-specific threshold defined by CBG, where if the bank's debit position exceeds that limit, all cheques presented on that bank will be put on hold until the bank's debit position is reversed. The returned/rejected cheques, though would worsen the net position but must be done.

4.8 Early Cheque Items

The CIS daily operations shall start the clearing session for a clearing day at the 1st cut-off time of the previous business day's regular clearing session. (Refer to Rules 4.2.1 and 4.5) This is to provide an earlier time for participants to submit cheques as **'early items'** for the next business day clearing session.

CBG shall accept any cheque presented after 14:30pm (1st cut off time of regular cheques) and schedule them for clearing to the next business day. CBG reserves the right to alter the start and end times of the early items session. Participants shall be notified of any changes to the session times via messages over electronic media or other appropriate means.

4.9 Settlement via RTGS

CIS shall prepare all replied cheques, (which are confirmed to be paid by Issuing Bank or returned/rejected) and those auto-accepted, for settlement at the end of each clearing session. CIS shall perform multilateral netting of all confirmed cheques for all participants, and prepare a **Net Clearing Position (NCP)** file. The CIS shall submit the NCP file to the RTGS system at the end of each clearing session (this applies in both the regular and special clearing) for settlement of funds between the Presenting Bank and Issuing Bank accounts.

4.10 Authority of CBG

CBG shall have the following authority in the daily operations of the CIS:
- Controlling the installation, maintenance "including updates", operations, security, and contingency arrangements for CIS and the telecommunication links connecting to CIS between the Central Bank and the Participants:
- Day-to-Day control over the management and operation of the Central System;
- The Management of systems capacity and telecommunications traffic;
- To regulate, administer and monitor CIS.

CBG shall monitor the activities of each participant electronically and by physical inspection to ensure operation strictly in accordance with these Operational Rules and to control operational risks.

Hannibal-TelecompAdmin is an administration module installed in the clearing house for managing the clearing system as follows:

- Managing operation settings.

- Managing of the reference frame of the clearing system (updating, generation, sending to banks).

- Displaying query execution.

- Statistics production

- Setting control and clearing rules.

- Electronic Key management (reception, generation, sending to banks) etc.

5. RULE 5 – CHEQUE STANDARDS

All personal cheques and company cheques in The Gambia are eligible for clearing by the CIS. The cheques submitted to CIS must comply with standards as described in the following:

5.1 Cheque Currency

Cheques in different currencies will be identified by the Currency Code shown on the MICR line.

The imaging system should be able to process local and foreign currency cheques in separate batches by using the same set of hardware and software. Operating procedures should largely be the same. There should not be any dependency or conflict between the processing of cheques of different currencies. The imaging system should be capable of alerting the operator if cheques of different currencies are mixed in one batch.

5.2 Cheque Size

The imaging system should be able to handle a cheque amount field with a maximum of 17 digits before the decimal point and 2 digits after the decimal point. Cheques size must also conform to the West African Monetary Zone (WAMZ) Cheque Standards as specified in Section 5.3 below.

5.3 Paper Specifications

The cheque dimensions and weight must meet the following specifications, categorised into Small or Large Cheques:

Cheque Type / dimensions	Small cheque	Large cheque	
		Manual infill	Computer Infill
Length	$6^{7/8}$ inches / 174.6 mm	$6^{7/8}$ inches / 174.6 mm	$8^{1/4}$ inches / 210 mm
Height	$2^{7/8}$ inches / 73 mm	$3^{7/8}$ inches / 99 mm	$3^{7/8}$ inches / 99 mm
Grammage	95 gram ± 5%		

Tolerance: ± $^{1/16}$ inch (1.6 mm) vertically and ± $^{1/20}$ (1.3 mm) horizontally

5.4 MICR Line Standards

Summary of MICR line information in the image and data file of a cheque.

The pre-coded MICR line information to be supported is:
- Bank code (minimum 3 characters)
- Branch code (minimum 4 characters)
- Cheque serial number (minimum 6 digits)
- Account number (minimum 20 alphanumeric characters)
- Check digit (minimum 2 digits)
- Currency code (3 digit ISO 4217 standard)

The post-coded information for the MICR line is:
- Amount (17 digits)
- Date (8 characters, i.e. DDMMYYYY)
- Transaction code (minimum 2 chars)
- Serial number (minimum 7 digits)
- Clearing Centre code (minimum 2 chars)

5.5 MICR Specifications

The MICR line specifications are as detailed below:

Order	Name	Starting Position	Length	Description
1	Cheque Number	2	08	
2	Drawn Country code	11	02	01 (GM) /05 (SL) / 03 (GN)
3	Drawn bank code	13	03	
4	State code	16	02	
5	Drawn branch code	18	03	
6	Account number	22	10	
7	Account number Check digit	32	02	Modulo97 : include the bank code, branch code and the account number
8	Transaction code	35	02	01 : Personal cheque 02 : Corporate cheque 03 : Bank Draft
9	Currency code	37	03	270 (GM) /694 (SL) / 324 (GN)
10	MICR Check Digit	40	02	Modulo97 include all MICR digits (35 digits)

5.6 Cheque Images Format

Attributes of the cheque image format to be used in the imaging system should not be lower than the following standard:

> Compression: JPEG
>
> Grey scale: 256
>
> Resolution: 120 dpi

5.7 Non-standard Cheques

Any cheques not in compliance with the above standards may be rejected by the CIS.

6. RULE 6 – OUTWARD CLEARING

The participant as Presenting Bank must perform the following steps in the outward clearing of cheques deposited by their customers:
• Electronic scanning of cheques
• Data Entry for cheques captured
• Quality Assurance & Repair (if necessary) of cheques
• Balancing and presentment of cheques.
The rules for participants to follow in each step are described as follows:

6.1 Scanning of cheques

The Presenting Bank must designate staff to perform scanning of cheques using the certified CIS scanners to capture electronic images of the cheques, as well as the MICR line data. The participant must create cheque batch and add the scanned cheques to batch.
Multiple cheques can be scanned where they are grouped inside batches. The participant must create batch for grouping cheques with the following common information:
• Presenting Bank
• Presenting Bank Branch
• Payment Method
• Presenting Bank Account Number
• Depositor Name
• Reference Name
• Currency name
• Urgency

The system shall allow users to upload the current batch and all existing batches to the server. The system shall prevent uploading duplicate cheques. It shall also prevent users from uploading unbalanced batches. The system shall handle duplex cheque scanning (face and back sides scanning) using duplex cheque scanners.

It is the responsibility of the Presenting Bank to examine all physical cheques before scanning the cheques into the system. The Presenting Bank designated staff for

scanning must act on behalf of cheque issuing bank by checking the cheque genuineness and the cheque compliance to the CIS operating rules, before he/she scan the cheque. The Presenting Bank staff must not accept any fraudulent cheques or any of the following:

- counterfeit cheques;
- copies of original cheques;
- any cheque with an embedded photo-copy information;
- Cheques already processed and Cleared/Accepted
- Rejected cheques for which reasons for the rejection remain unchanged

If the Presenting Bank staff is uncertain as regards genuineness, (e.g. 'suspicious cheque'), the bank must alert the Issuing Bank for further verification. The Presenting Bank shall become liable if counterfeit or abnormal cheques are scanned into the system and processed. CBG shall apply severe penalties and/or disciplinary action in such cases.

6.2 Data Entry

Designated staff of the participant must perform data entry for completing and balancing the batch and scanned cheques information. The following information must be completed and entered by participant, where necessary, at the data entry stage:

- Cheque amount
- Cheque Date
- Presenting Bank account number for depositing cheque amount
- Any correction to the MICR line (if it has not been successfully captured in the scanning process)

6.3 Quality Assurance

The Presenting Bank must adopt its internal auditing procedure for performing quality assurance of cheques captured into CIS. The Presenting Bank must designate a different staff at supervisory level compared to the cheque scanning staff, to perform the quality assurance check function in the system. This shall ensure that a proper dual control is applied.

The quality assurance system flow includes the following steps:

1. The Quality Assurance (QA) staff examines batch/cheques for the following criteria:
   - Confirm the date on the cheque
   - Confirm the amount in word and number
   - Confirm if there is alteration and endorsement on cheque
   - Confirm the face and back of cheque image and compare it with physical cheque
   - Confirm if the physical cheque is genuine (not counterfeit)
   - If cheque looks suspicious, the quality assurance staff must select the option of "physical paper required" or similar command for the Issuing Bank to confirm authenticity

• Confirm the MICR line against captured data
• Confirm that the data entry or repair has not incorrectly changed the MICR data compared to the MICR line
• Confirm the quality of image

2. If batch/cheque contents pass the QA criteria, the user elects to approve the batch

3. If batch/cheque content doesn't pass the QA metrics, the user elects to repair the batch.

It is the responsibility of the Presenting Bank to ensure that the quality assurance resulted to the best possible check on the correctness of the presented cheque information, including the captured MICR line data which may have been repaired due to reasons such as an error in image capture. If CBG identifies that the Presenting Bank has caused an incorrect MICR data to be sent to the system, CBG may impose a penalty charge or institute disciplinary action.

6.4 Cheque Repair

Cheque image capture may be rejected because of poor quality images. The imaging system will allow the user to repair or enhance the image quality of captured cheques. The endorsement sequence number, index of cheque images and registers for reconciliation should be updated if re-capture is required. The workflow should not be severely disrupted.

The participant staff must perform the repair function to correct all errors found in the cheques after processing them through the quality assurance step. When the repair is completed, the participant staff must dispatch repaired batch for performing QA confirmation again.

6.5 Inquiry of Replied Batches

The CIS enables participants to inquire replied batches which were sent from Issuing Bank to Presenting Bank. The replied batches information identifies cheques which are accepted by the Issuing Bank and cheques which are rejected.

Presenting Bank user should either send those rejected cheques to the repairing phase, or to represent them to the CIS after the reason(s) for rejection is/are addressed.

6.6 Cheque Stamping

Presenting Banks will apply a stamp at a designated location on the back of each outward clearing cheque before generating its image. The stamp will bear the name of the bank, the word "Clearing" and the date of presentation.

The imaging system will allow user customisation for changing the location on the back of the cheque where the clearing stamp is to be applied.

The imaging system is capable of marking an identifier in the index of the cheque image during the image exchange process to denote that it has been cleared by the Clearing House and the date of clearing.

If a cheque has been replied accepted by the Issuing Bank, the Presenting Bank must stamp the replied cheque with **"Cleared/Accepted"** at the front. This will give a detailed track of cheque presentation cycles and its acceptance date.

If a cheque is rejected by system or returned by Issuing Bank, the Presenting Bank should stamp or mark it as **"Rejected/Returned"** at the front of the cheque.

In case of cheque representation, the Presenting Bank shall stamp a new date at the back side of the physical cheque. This shall give a detailed track of cheque presentation cycles.

6.7 Cheque Endorsement

Banks should apply an endorsement sequence number at a designated location on the back of each outward clearing cheque before generating its image. The endorsement sequence number of each cheque should be part of the index of its image record.

The endorsement format sequence number is for easy reference such as the following:
- YYYYMMDDBBBRRRRNNNNNNN, where
- YYYY is the century information,
- MMDD where MM is the month in digits and DD is the day in digits.
- BBBRRRR is the capture point, with 'BBB' as the bank code, and 'RRRR' as the branch code where the cheque is captured, and
- NNNNNNN is the sequence number.
-

The imaging system should allow the system to change the location on the back of the cheque where the endorsement sequence number is to be applied. The position will be standard for all banks and individual bank participants.

6.8 Cheque Representation

Presenting bank may resend a rejected cheque to CIS for re-presentation, if the Presenting bank believes the exception which caused the earlier rejection has been addressed.

A cheque which needs to be resent to CIS must only be represented from the same Presenting bank which initially presented it to CIS. The system shall reject the representation if not done by the original presenter.

6.9 Deposit Advice Printing

Presenting bank user may print a Deposit Advice from CIS for a cheque which has been replied as accepted by the Issuing Bank. The Presenting bank can forward the deposit advice to the depositing customer for reference.

6.10 Return Advice Printing

Presenting Bank user may print a Returned Cheque Advice from CIS for a cheque which has been rejected by the Issuing Bank as returned cheque. The Presenting bank can forward the returned cheque advice to the depositing customer for reference.

6.11 Special Handling Cheques

Special handling cheques are cheques that the Presenting Banks consider necessary to be physically exchanged such as:
- Suspected fraudulent or counterfeit cheques
- Cheques with no magnetic effect detected during MICR capture
- Bank drafts
- Copy of lost or mislaid cheques.

The system allows users to classify a cheque into the category of special handling cheque during the capture and data entry process.

If the Presenting Bank identifies a deposited cheque as suspicious and would like to request the Issuing Bank to confirm the cheque, the Presenting Bank user should flag the cheque in CIS as special handling required. The CIS will transmit the cheque information together with this message to the Issuing Bank.

If Presenting Bank does not send the physical cheque to the Issuing Bank under such circumstances, the Issuing Bank may return the cheque / send it back to the Presenting Bank.

7. RULE 7 – INWARD CLEARING

The participant as Issuing Bank must perform the following steps in the inward clearing of cheques sent from CBG CIS to the participant:
- Technical Clearance of cheques
- Financial Clearance
- Clearing Approval of cheques
- Return of rejected cheques

The rules for participants to follow in each of these steps are described below:

7.1 Technical Clearance

Issuing Bank participant must designate staff to perform Technical Clearance of cheques against a specific technical checklist. The technical checklist must include, at a minimum, the following items:

a. Confirm the cheque signature against paying customer's signature;
b. Confirm whether the amount in words and figures tally;
c. Confirm that cheque alternations are countersigned;
d. Confirm that the cheque date is the same as or before the current business date;
e. Confirm whether the cheque is stale (out of date);
f. Confirm the MICR line on the cheque image against data captured;
g. Confirm whether the cheque is drawn on the Issuing Bank;
h. Confirm the authenticity of the cheque image;
i. Confirm whether the cheque requires specific handling;
j. Confirm whether the cheque is a stop cheque;
k. Confirm whether the physical cheque requires examination.

The Issuing Bank participant must pay attention if the different MICR line data captured, such as Issuing Bank number, branch code, account number, are different from the MICR line on the image. This could have occurred due to one of the following reasons:

- Presenting Bank has modified/repaired any one of the MICR data fields after they are captured.
- The MICR line was not correctly captured due to the physical MICR line quality, and the quality assurance of Presenting Bank failed to detect.

Under such circumstances, the Issuing Bank participant clearing staff should analyse and make decisions if the cheque is drawn on the correct participant, branch or account; and thereafter accept or reject the cheque.

It is the responsibility of the Issuing Bank to ensure that their clearing staff has done the best possible verification of the MICR data captured against the MICR line on the cheque image. If the Issuing Bank has failed to detect an error in the MICR data captured, the Issuing Bank shall be responsible for any financial loss or complaint on the cheque payment caused by the error.

7.2 Financial Clearance

Issuing Bank staff must perform financial clearance of incoming cheque by verifying against the following financial checklist:
a. Confirm whether the paying customer's account has sufficient funds
b. Confirm whether the account is not blocked or closed

7.3 Clearing Approval

Issuing Bank must designate an appropriate staff to perform Clearing Approval of a cheque, after the technical and financial clearance steps are completed. The clearing approval Officer must decide the action for the cheque and send reply to the Presenting Bank whether:

- Approval of cheque for subsequent payment to Presenting Bank, or
- Rejection of cheque with valid reasons.

7.4 Stop Pay Cheques

The CIS provides an option to maintain a 'Stop Cheque' table which defines the types of cheques to be rejected from clearing. The 'Stop Cheque' information should include the following:

- Cheque number information for cheques which have been reported lost (owner bank code, branch code, cheque number)
- Account number of drawer which has been blacklisted for clearing
- Any other flexible parameters for defining the stop criteria of a cheque

If the CIS receives an outward cheque which matches the stop criteria, the system will reject the cheque in the submission file and send an alarm message to the presenting bank.

The CIS system will also generate an alert message for each stop cheque received. The Clearing House administrator should be able to inspect the list of cheques stopped with the associated information of issuing banks and account owners.

The Issuing Bank may define a list of stop pay cheques in the CIS. The CIS shall verify if any inward clearing cheque matches any details in the stop pay list. If a match is found, the system shall tag the cheque with a warning message to alert the Issuing Bank.

7.5 Positive Pay Cheques

The Issuing Bank may define a list of positive pay cheques in the CIS. The CIS shall verify if any inward clearing cheque has a match with the positive pay list. If a match is identified, the system shall tag the cheque with an information message to notify Issuing Bank clearing Officer at the technical clearing and financial clearing stages.

The Issuing Bank shall be responsible for the final decision to approve the cheque with the 'positive pay matched' message and for any addition or correction to the positive pay cheques list in the CIS.

8. RULE 8 – CHEQUE RETURN PROCESSING

The T**elecompAdmin** allows defining and codifying all operations' rejection reasons that will be used by participating institutions.

The entered data are:

- Rejection code.
- Rejection motive or reason.

Examples of possible return reasons are detailed below:

(a) System Return Reasons:

The system return reasons will be used by the system to reject a cheque automatically on behalf of the Central Bank, due to errors or exceptions identified on the cheque.

(b) Issuing Bank Return Reasons:

The Issuing Bank may return cheque for technical and financial reasons as follows:

However, each time a cheque is returned for applicable reasons, the CBG shall count this as part of the allowable presentations per cheque **(maximum number of three times allowed)**. If countable presentations are 'Y' i.e. YES: this means that the reason will be considered when counting the number of presentation cycles for the cheque, but if it is 'N' i.e. NO then it will not form part of the presentation cycle.

8.1 System Return Reasons

The system return reasons shall be used to reply to cheque(s) that is/are rejected due to a certain system reasons based on the cheque details.

The following table describes the list of possible system return reasons:

Return Reasons	Purpose	Countable Reason
No available session/ Inactive system	This reason applies when rejecting the cheque automatically if the Presenting Bank tried to send a cheque outside the available presenting period or when the daily clearing session is not available.	N
Bank Suspended	This reason is used to reject the cheque automatically if the Presenting Bank or Issuing Bank has been suspended.	N
Destination Unreachable	This reason is used to reject the cheque automatically if the Presenting Bank sent a cheque to CIS, and CIS has performed the maximum number of retries in attempting to send the cheque to the Issuing Bank (destination) without being able to deliver the cheque, then it will send an automatic reply that the cheque is rejected due to a problem in the communication	N
Different Presenting Bank	This reason applies when rejecting the cheque automatically from the CIS due to its presentation from two different banks.	N
Cheque already paid	This reason applies when the Presenting Bank tries to send a cheque that has already been accepted / paid.	N
Exceed re-presentation	This reason applies if the Presenting Bank has exceeded the maximum number of presentation times. The number	N

count	of presentation times for each cheque shall be determined by CBG from time to time.	
Session Terminated	This reason applies if a cheque is presented after the termination of session	**N**
Bank Defaulted	This reason applies when the cheque is presented from or to a bank that has been in default of other settlements.	**N**
Bank Terminated	This reason applies when the cheque is presented from or to a bank that has been suspended/terminated.	**N**

8.2 Issuing Bank Return Reasons

The following table is the list of Issuing Bank return reasons (technical and financial reasons) which may be used by participants:

Return Reason	Purpose	Countable Flag
Insufficient funds	This reason shall be used when the available balance of the customer pay account number is not sufficient to make the cheque payment.	Y
Refer to Drawer (Other Than Insufficient Funds)	This reason shall be used by technical clearing user if the cheque matches with a stop cheque as instructed by the drawer customer; in which case the Issuing Bank needs to contact the drawer customer to determine if the stop cheque is a valid reason for return of cheque.	Y
Stale cheque (out of date cheque)	This reason shall be used by the technical clearing users when the Issuing Bank decides not to honour a cheque which has exceeded the maximum period defined in the system.	Y
Post Dated/ Undated	This reason shall be used by the technical clearing user when the Issuing Bank receives a cheque which is either post dated or undated. Post dated cheques should be held in the Post Dated Cheque system of the Presenting Bank and not sent to Issuing Bank until the due date.	Y
Payee's Name Required/ Payee`s Endorsement Irregular	The reason applies when the payee's name on the cheque is not clearly identified.	Y
Stop Pay Cheque	This reason is used in financial clearing to reject the cheque which has been added on the stop cheque list, and/or	Y

	when it is reported as a lost cheque.	
Alteration - Requires Drawer's Confirmation	This reason is used by the technical clearing users to reject the cheque when it is edited without approval by the drawer.	Y
Amount in words and figures differ	This reason is used in technical clearing to reject the cheque, when the amount in words doesn't match the amount in figures.	Y
Cheque Not Drawn on us	This reason is used by the technical clearing users, to reject the cheque in case it has been presented to a wrong destination bank. This case can happen rarely if the MICR line (especially the bank code) of the cheque has been read incorrectly, and the Presenting Bank is responsible for this fault.	N
Drawer's Signature Required/Differs/Addition Signature Required	This reason is used in technical clearing when there is missing signature, or the signature on the cheque doesn't match the signature on the banking system or when the signature on the cheque doesn't match the customer counter signature on any alteration made on the cheque.	Y
Account Closed/Transferred/Frozen	This reason is used in financial clearing when the drawer's account is closed, transferred, or in frozen status.	Y
Drawer Reported Deceased	This reason is used in financial clearing when the drawer has been reported deceased.	Y
Special handling cheque not received	The reason is used when the inward cheque image record is marked for 'special handling required' but the Issuing Bank has not received from Presenting Bank the physical cheque for examination.	Y
Court order not to pay check	This reason applies for rejecting cheques when there is a restriction on the cheque by the courts..	Y
Account number doesn't belong to drawer/ the cheque isn't related to the client	This reason shall be used for rejecting the cheque due to the inconsistency in the account number and its owner. This case might happen if the teller at the Presenting Bank didn't notice the error when scanning the cheque, or when	Y

	he/she edits the account number of the MICR wrongly.	
Drawer bankruptcy	This reason applies when rejecting a cheque drawn by a bankrupt drawer.	Y
Difference between check image and data/Data and image mismatch	This reason is used by the technical clearing users when the teller or the user at the Presenting Bank has entered incorrect data (such as: Amount, or date) as compared to the cheque data.	Y
Recall by Presenting Bank	This reason is used by the technical clearing users when the Presenting Bank informs that the cheque is incorrectly presented, and should not be paid by the Issuing Bank.	Y

8.3 Obsolete Return Reasons

As the cheque clearing operations are conducted through online cheque images and electronic data, the exchange of paper cheques for daily clearing is no longer required. The following return reasons which are applicable only in the paper cheques environment shall not be applicable in the CIS operations:

Reasons to become obsolete	Justification
Mutilated cheque/ Envelope	The use of envelope for return cheques and non-MICR cheques are not required anymore since cheques are exchanged electronically and return cheques are sent online from Issuing Bank to the Presenting Bank.
Other returned reason	This should not be used in order to avoid misuse by Issuing Bank and cause delay or non payment to an inward cheque without an approved reason.
Crossed by 2 Bankers/ Cancellation of Cross Stamp Required	Stamping on the cheque shall not be provided to Issuing Bank, since the physical cheques will not be exchanged with the Issuing Bank. The cheques received by the Issuing Bank shall have been endorsed by the Presenting Bank after it has completed data entry and quality assurance steps.

8.4 Return Cut-off Time

The Issuing Bank shall observe the cut-off time defined for returning cheques in each clearing session. The CIS shall not accept any return cheques which are sent by Issuing Bank participants after the cut-off time of the respective clearing session for the original cheques.

8.5 Recall of Cheque

Once Presenting Bank participant presents a cheque which has been accepted by CIS, the participant is not allowed to recall the cheque and cancel it for clearing.

If Presenting Bank needs to recall a cheque because it has been presented to CIS by mistake, the Presenting Bank should contact the Issuing Bank and request the Issuing Bank to return.

8.6 Incorrectly Presented Cheques

If Presenting Bank participant identifies that he has incorrectly presented a cheque and the cheque is accepted by the CIS, the participant should immediately contact CBG to request its cancellation. This must be performed before the participant presents the correct cheque which has the same MICR line information. Otherwise, the CIS shall handle the second presentation as a 'duplicate' cheque.

8.7 Return Cheque Advices

When the Issuing Bank returns a cheque with a valid reason within the cut-off time limits of the clearing session, the CIS shall forward the return cheques to the Presenting Bank for their attention or action.

The CIS provides a Return Cheque Advice function for enquiring and printing returned cheques. Presenting Bank shall be able to print the Return Cheque Advice which provides a record for the cheque image and the return reason. The Returned Cheque Advice shall be used by the Presenting Bank as the sole advice and evidence of returned cheque for providing to the cheque depositing customer. Any other advice or cheque images, which are not produced from the CBG CIS, shall not be used by any participant for providing to the cheque depositing customers as evidence of returned cheque.

9. RULE 9 – SETTLEMENT OF CLEARING

9.1 Time of Settlement and settlement schedule

CIS shall perform multilateral net settlement of cheque payments amongst participants by sending the net settlement result to the RTGS system.

Net settlement will be carried out at the end of each clearing session. Multiple net settlements will be performed for special clearing cheques (once for each special clearing session). A single net settlement for regular cheques shall be performed each day after the regular clearing session for clearing business day ends.

The normal daily schedule for CIS to commence settlement process with RTGS shall be as determined in Section 4.5. CBG reserves the right to modify the number of times of

settlement and their time schedule within each business day depending on the operational situation and to notify Participants accordingly.

The CIS shall generate Net Clearing Position (NCP) file for each net settlement. The NCP shall adopt the SWIFT MT971 message format. The CIS shall send the NCP via MT971 message to RTGS system.

9.2 Settlement Process

The process of settlement of NCP with RTGS shall follow the message flow in the following diagram:

Figure 3: Net Clearing Position Settlement flow
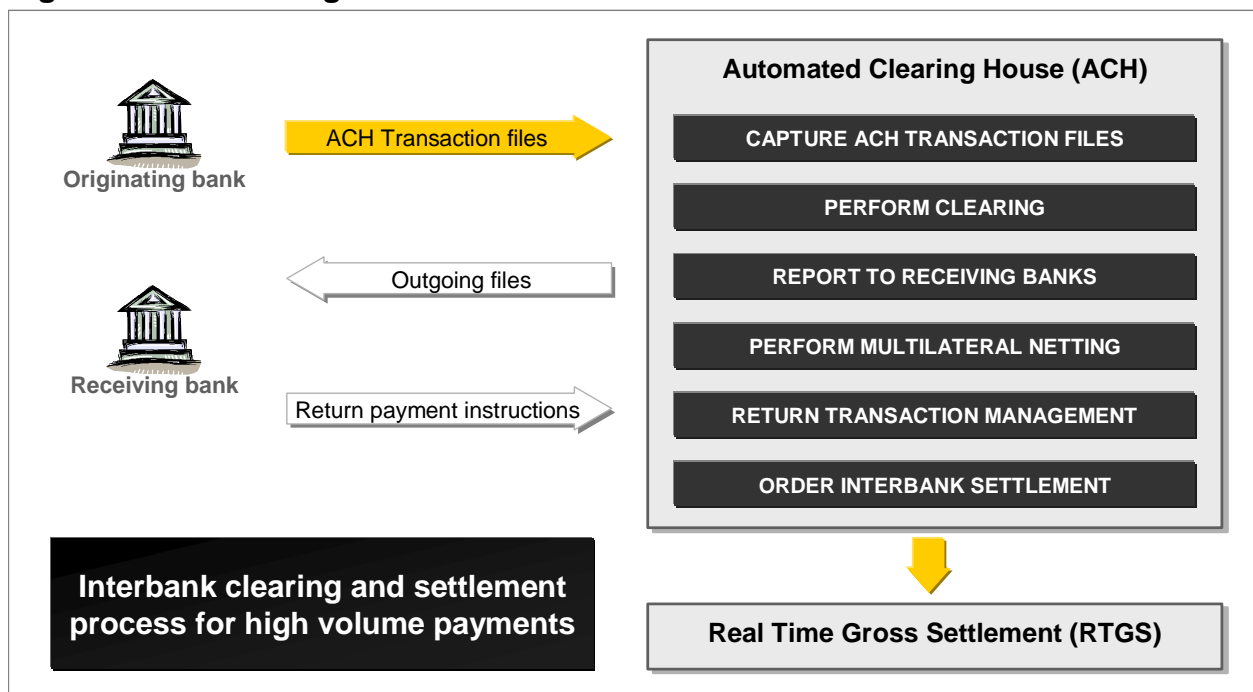
(Step 1) During exchange window of RTGS, the CIS submits an MT971 Message containing the Net position of Participants (credit or debit)
(Step 2) RTGS validates this message and issues an error notification if it didn't pass through validation procedure
(Step3) If the validation is successful, the message is presented to Settlement as Net transaction.

RTGS checks the availability of funds in Participants' Accounts with Net debit positions and, once funds are available, debit and credit the Accounts of clearing Participants on an "all-or-none" basis. In case of lack of funds on any account, Net transaction is queued.

If there are no sufficient funds to settle Net transaction on Settlement account(s), RTGS notifies Participant(s), to cover their Debit positions. This message contains Net Debit position and Available balance on the Settlement account.

9.3 Notification of Settlement

When net settlement is successfully performed by the RTGS system, each participant in the respective NCP settlement list shall receive from the RTGS system appropriate debit/credit notification (i.e. MT900/MT910 messages) for the debit/credit transactions effected on the participant's settlement account.

9.4 Failure of Settlement

If the net settlement cannot be performed because one or more participants cannot fund their settlement account, CBG may offer the following options:
- The failing participant borrows funds from the interbank market;
- The failing participant requests for liquidity via **Intra-day Liquidity Facility (ILF)**. The options have to be explored and chosen by the defaulting bank(s) within the settlement session.

10. RULE 10 – FINALITY OF PAYMENT

10.1 Definition of Finality

When the settlement of Net Clearing Positions (NCP) in the RTGS completes successfully, all the cheque payments which are included in the NCP file are deemed 'final'. Net settlement in RTGS system shall be irrevocable. Finality of settlement shall also apply under specific circumstances, as may be stipulated by the CBG.

10.2 Obligations of Participant

Once payment of a cheque is deemed final at the end of its clearing cycle, Presenting Bank is obliged to pass credit of the cheque value to the beneficiary customer of the cheque. The participant shall value the credit to the beneficiary as soon as possible at the same day when the cheque finality is reached.

10.3 Return of Funds

Once a CIS cheque payment is settled via RTGS to conclusion, any request from the Issuing Bank for return of funds on behalf of their customers should be handled outside the CIS.

If a net settlement transaction for a participant has been finalised in RTGS but later found to be erroneous, the participant is obliged to contact the counterpart involved in the transaction. The two participants should seek mutual agreement on the appropriate method of resolution. Any payment used for the resolution between the two participants should be seen as a new transaction and does not change the irrevocability of the previously completed net settlement transaction.

11. RULE 11– SYSTEM INTERFACES

11.1 Interface with Core Banking Application

Participants shall develop system interfaces between their core banking system and the CIS. The system interface shall provide the outward cheque data file and inward cheque data file which contains the cheque transactions ready for posting to the participant's core banking system.

At the clearing house level, the settlement files will be forwarded to the RTGS at a specified time during the clearing cycle.

RTGS will carry out simultaneous irrevocable settlement between the banks, and update the settlement accounts in the **Central Bank General Ledger**. Normally this is a two-stage process:
- the first stage is to ascertain that sufficient funds are held;
- the second is to debit or credit the bank's settlement account.

In the event that a bank is unable to meet its settlement obligation, the settlement will be cancelled in the RTGS and the transactions returned to the ACH system where they must be unwound and cancelled. Otherwise the system automatically communicates settlement data from the RTGS system to the Core Banking Application (Terminus T24).

11.2 Inward Clearing File Interface

Inward cheque image files are forwarded to the issuing bank at each clearing session. The system supports multiple deliveries of inward cheque images during the clearing session to the participants.

Each participant bank is able to receive the following types of files at the ACP Front End system:
- Inward cheque images and MICR-encoded information for verification at the issuing bank.
- Inward return cheques with reason codes
- Reports and reconciliation totals.

Inward Cheque Information
The inward clearing function at the ACP Front End system allows the bank staff to perform the following:
- View the image of an incoming cheque and check the details for any technical errors or missing information as follows:
  - Front and back of cheque image
  - Presenting bank and branch
  - Drawee's account number
  - Amount
  - Date
  - Drawee's signature
- A supervisory approval function is available to provide dual control on clearing inward cheques.

12. RULE 12 – REPORTS

12.1 Outward Reports

The CIS shall provide the following data reports to all Participants:
- Outward Summary Report
- Presented Cheques by Presenting Bank Branches
- Presented Cheques by Issuing Bank
- Detailed Presented Cheques
- Honoured Cheques by Presenting Bank Brach
- Honoured Cheques by Issuing Bank
- Detailed Honoured Cheques
- Returned Cheques by Presenting Bank Branch
- Returned Cheques by Pay Branch
- Detailed Returned Cheques
- System Returned Cheques by Presenting Bank Branch
- System Returned Cheques by Issuing Bank
- Detailed System Returned Cheques
- Destination Unreachable Cheques by Presenting Bank Branch
- Destination Unreachable Cheques by Issuing Bank
- Destination Unreachable Returned Cheques
- No Session Available Returned Cheques by Presenting Bank Branch
- No Session Available Returned Cheques by Issuing Bank
- Detailed No Session Available Returned Cheques
- Waiting Cheques by Presenting Bank Branch
- Waiting Cheques by Issuing Bank
- Detailed Waiting Cheques
- Auto Replied Cheques by Presenting Bank Branch
- Auto Replied Cheques by Issuing Bank
- Detailed Outward Auto Replied Cheques

12.2 Inward Reports

The CIS shall provide the following data reports to all participants:
- Inward Summary Report
- Received Cheques by Pay Branch
- Received Cheques by Presenting Bank
- Accepted Cheques by Pay Branch
- Accepted Cheques by Presenting Bank
- Rejected Cheques by Pay Branch
- Rejected Cheques by Presenting Bank
- Pending Cheques by Pay Branch
- Pending Cheques by Presenting Bank
- Detailed Pending Cheques
- Auto Replied Cheques by Pay Branch
- Auto Replied Cheques by Presenting
- Detailed Inward Auto Replied Cheques
- Net Clearing Position

12.3 Outward & Inward Management Reports

The CIS shall provide the following data reports to all participants:
- Presented and Rejected
- Received and Returned
- End of Session Reconciliation Report
- Presented and Returned Statistics Report
- Received and Rejected Statistics Report
- Bank Returned Statistics Report
- Bank Rejected Statistics Report
- System Returned Statistics Report
- System Rejected Statistics Report
- Technical Returned Statistics Report
- Technical Rejected Statistics Report
- Financial Returned Statistics Report
- Financial Rejected Statistics Report
- Auto-Accepted Statistics
- Net Clearing Position Details by Session
- Net Clearing Position Details for all Sessions
- Net Clearing Position Summary by Session
- Net Clearing Position Summary for all Sessions

12.4 Online Inquiry

The CIS shall provide the following information available for online inquiry by all participants:
- Master Exchange Query of cheques presented by and to the banks
- Historical Query of Cheques

13. RULE 13 – SECURITY CONTROLS

13.1 Cryptography Security

For the protection of Participant's system against every non-authorized access and avoid network intrusions, it is recommended to:
- Subdivide its network in groups of DMZ, in order to protect servers and data sources by Firewall use (filter all incoming and outgoing connections).
- Use hardware probes to detect network intrusions
- Use software probes on production servers to stop all intrusion attempts into the servers.
- Use an antivirus in the servers and the workstation.

The main functionality of **Barberousse-GenerateurCles** (Head Office Key Generator) is to provide signature authentication and encryption keys that are needed to secure images. These keys are transmitted to the branch by **Barberousse-GenerateurCles** of the bank's head office through the SSL protocol. It operates at head office mode, but also in every scanning location, in the branches.

The system shall encrypt and validate the authenticity of all cheque images and cheque data by the following:

> • Encrypted cheque image shall be verified via decryption using **Symmetric Algorithm DES:** (Triple DES key).
> • MICR line data shall be validated based on standard safeguards against any possible counterfeit.

13.2 Authentication

The CIS identifies and authenticates each user interacting with the system, including designated users from Participant or CBG, by verifying the identifier that is being used and the password.

The information about user logons/logoffs or incoming and outgoing messages is stored in the database with associated timestamps, physical source identification as well as the acknowledgement message of the system.
.
A **forced logoff facility** after a certain period of inactivity (time out) shall be used by participant. The maximum duration of an idle period is configurable either by the Participant or System's administrator.

The system shall support authentication of logon by the participant using directory services. The system shall support three levels of authentication:
- Local Participant User Level – authentication check will be performed based on the domain security built in the operating system of CIS;
- Inter Process Level – authentication at the level of the system core services;
- Inter Site Level – authentication at the level of the data exchange between two workstations.

13.3 User Management

CBG shall perform user management function to add or delete users to the system. The user management function also defines or modifies the following attribute of users:
- User account lock;
- User allowed working hours on the system;
- User membership group;
- User membership role;
- User workstation;
- Directory user setting.

13.4 Group Management

The system shall allow defining User Groups for each participant. The Group Management function of the system performs the following:
• Add/delete/modify/list Group definition
• List of user members to the Group

13.5 Role Management

Upon authenticating the user, the system shall authorize the user to access certain functionality depending on his assigned role. The system shall provide Role Management function for participants to perform the following:

• Add/delete/modify/list Roles definition
• List of privileges definition within a Role
• List of user members to the Role

13.6 Access Control List (ACL)

The CIS shall maintain Access Control List (ACL) to define the list of authorized functions for each user in Participants and CBG organization. User cannot access any other function which is not allowed in the ACL.

The CIS ACL management function shall also define the list of branches for each participant and the access control privileges on branches users.

CBG system administrator shall have the right to define the access privilege of users of each participant. CBG system administrator shall perform the following responsibilities:

    • to distribute responsibilities according to type of Participant and User of Participant within CIS;
    • to assign Access Rights for each Participant independently and according to his role in the system;
    • to adjust Access Rights for each Participant independently;
    • to change Access Rights assigned to Participant where necessary;
    • to audit Access Rights previously assigned to Participants.

13.7 System Administration

CBG shall perform administration of security policies to which participant users must comply with. CBG shall have the right to modify the security policies depending on operating environment, and shall advise all participants accordingly.

The security policies of system shall include the following:
    • complex password rules which include:
        - password expiration period
        - minimum password length
        - password mask complexity
    • password history
    • list of application components configured on the system
    • list of workstations configured on the system
    • Directory Services Setting

CBG Systems Administrator and Management shall have access to the following Reports

- Daily ACP incoming/outgoing data transactions including reconciliation and returns (date stamped sent and received)
- Accepted payment summary
- Payment captured report
- Branch listing of ACH transactions
- Statement of ACH transactions
- Daily ACH summary by account and volume
- Daily payments clearing summary
- Rejected item report
- List of returned transactions by returning bank
- Returned transaction summary by returning bank
- ACH return reversal summary
- Statistics of returned items
- Net Settlement Report
- Processing times and performance statistics
- Capacity analysis
- Journal
- Operations log

13.8 Audit Log Management

The system shall record audit trail records for each and every action performed by the users and the system.

Participants shall be allowed to export audit trails pertaining to their activities via an external file. Participants shall maintain proper backups of the exported external files for their own use.

13.9 Participant's Database Security

CBG shall maintain and monitor the security protection of the database information belonging to each participant in the central CIS system. The database security measures shall implement the following:

- User database access limited to authorized users only
- Database level integrity hashing
- Cheque Image encryption
- No participant is permitted to access information/database belonging to other participants.

13.10 Participant's Responsibilities

13.10.1 Password Security

CBG shall provide username and password to authorized users for access to the CIS. It is the responsibility of the participants to ensure that their staff shall apply strict code of conduct for protecting their usernames and passwords, and safeguard against compromise by unauthorized users at their ends.

Password management

Each user will have a valid password for a period defined in the settings. Once the password comes to expiration, the application invites the user to enter new password which should be different from the expired one. Two security levels of password setting are provided by the application:
- Standard Security Level: allowing free passwords setting for users.
- Enforced Security Level : Some security rules must be obeyed in password setting such as :
  - Minimum and maximum length of the password characters
  - Coexistence of numeric and alphabetic
  - Coexistence of Upper Case and lower case alphabets.

Each participating institution can choose the password security level to apply in its branches.

13.10.2 Anti-virus protection

Participants shall ensure and implement effective anti-virus protection on any computer equipment used for access to CIS. The participant's policy towards anti-virus shall include the following:
- Up-to-date anti-virus software must be installed and activated in all CIS workstations of participants.
- Regular update of virus signature files shall be performed to keep updated with any new virus or worm identified in the industry.

13.10.3 Physical Access Protection

All equipments must be set up in safe offices. It is recommended for Security perimeter locations to:
- Be protected against non-authorized persons. Only one door should give access to the computer room, and an access authorization must be granted by the security responsible.

- Have an office access system using cards, badges or biometric system administrated by a controlling software;

- Have a security camera system;

- Be protected against fire : doors must be anti-fire and fire alarms must be installed;

- Be under controlled temperature : 18° to 21°

- Have a permanent electricity supply and security system for equipments.

The protection must be effective and robust at all locations.

13.10.4 Isolation with External network

The central CIS is operated on **Barberousse Capture** system and participant's CIS workstations accesses through web communication. Participants must implement protection to ensure that the participants' access points to the CIS network are securely isolated from any other network within the participants' environment.

13.10.5 Fraudulent Cheque Verification

It is the responsibility of the Presenting Bank to examine, verify all physical cheques and reject any fraudulent cheques before performing cheque scanning in the system. The Presenting Bank staff designated for scanning must act on behalf of cheque issuing bank by checking the cheque genuineness and the cheque compliance to the CIS operating rules. In future, the physical cheque may be truncated at Presenting Bank and the Issuing Bank shall not receive the physical cheque for verification.

The Presenting Bank staff must not accept any fraudulent cheques for scanning into the system, including the following:
- counterfeit cheques;
- copies of an original cheque via any means;
- cheques with an embedded photo-copy information

If the Presenting Bank staff is uncertain as to the genuineness of any cheque (i.e. is suspicious), he/she must select the option raising notice to that effect during scanning, thereby sending an alert to the Issuing Bank for further verification. The Presenting Bank should then follow-up by delivering the original physical cheque to the Issuing Bank within the allowed presentation cycle of the cheque.

Participants shall bear full responsibility and shall be subjected to severe penalty and disciplinary action applied by CBG, for participating in the capture of any counterfeit cheques or non-genuine copies of cheques and presenting to the CIS.

14. RULE 14 – SPECIAL PROCESSING DAYS

14.1 Business Hours

See details of Start and end of day in Section 4.5 of these Operational Rules.

14.2 Scheduled Public Holidays

CIS operations shall not be available on public holidays in The Gambia, nor on Saturdays and Sundays.

All cheques presented as early items on the last working day before the public holiday, or on Saturdays shall be carried forward to the next working day for clearing.

14.3 Unscheduled Public Holidays

In the event of sudden declarations of Public Holidays in The Gambia, CBG shall determine when it is convenient to terminate all operations and advise Participants accordingly.

15. RULE 15 – CHEQUE DATES

15.1 Stale Cheques

The acceptance and processing for payment of stale cheques (more than 6 months) is prohibited under these rules.

15.2 Post Dated Cheques

The CIS shall support acceptance of Post Dated Cheques (PDC) deposited from customers to a participant. The system shall maintain PDC in a PDC database. When the payment date of a PDC is due, the CIS shall roll the PDC into the normal clearing cycle.

15.2.1 PDC Input to CIS

Presenting Bank shall perform the following steps for inputting the PDC to CIS:
- Scanning of the PDC via CIS cheque scanner
- Filling in the incomplete cheque information for PDC using the CIS Data Entry function.
- Quality Assurance (QA) by Presenting Bank supervisors to verify the correctness of PDC
- Repairing of PDC, where necessary in order to pass the quality control checks.

15.2.2 PDC Storage

CIS shall maintain a PDC Storage for safe-keeping of active PDCs. Presenting Bank shall be allowed to perform the following on the PDC Store:
- List cheques
- View cheque information.
- View cheque image
- Edit cheque information
- Advance the posting Date of PDC.
- Send PDC to CBG to be presented.

16. RULE 16 - DEBIT CAP MANAGEMENT

16.1 Setting up of Debit Cap

CBG shall maintain Debit Cap limit for each participant in CIS. The Debit Cap limit defines the maximum Intra Day Liquidity Facility (ILF) permissible for individual participants within a clearing session. CBG reserves the right to determine or modify the ILF based on CBG's predetermined criteria.

16.2 Monitoring of Debit Cap

The administration and monitoring of ILF shall be in accordance with predetermined rules for the operation of RTGS framework in The Gambia.

16.3 Debit Cap Exceeded at End of Session

If session presentation-time elapses when the Debit Cap of a participant is exceeded, CIS shall reject all those cheques which are held for presentation to the participant. The system shall return those cheques to the presenting participants with a system return reason.

17. RULE 17 – HANDLING OF PHYSICAL CHEQUES

17.1 Legalization of Cheque Images

Like other electronic payment system frameworks in The Gambia, the CIS shall be operated in accordance with the laws of evidence and appropriate laws on the admissibility of electronic cheques, bills of exchange etc in The Gambia.

For cheques which have been rejected, or returned to the Presenting Bank, the Presenting Bank shall return the physical cheques to the cheque payee customers. The Presenting Bank shall also print the Cheque Return Advice for a rejected/returned cheque from the CIS to show the reasons for return.

CBG shall require that only cheque images which are generated by the CBG CIS, and not other imaging systems, will be empowered with this legal recognition.

17.2 Cheque Truncation

The ACP system is an on-line image based cheque processing system which captures magnetic ink character recognition (MICR) data and images at the presenting banks. The cheque details and images are electronically delivered to the ACH via a data communication network. It incorporates an appropriate security infrastructure to protect the electronic information.

Once the cheque is encoded and data delivered to the ACH, cheque processing is similar to other low value payments clearing. Netting and settlement is performed by the ACH system and RTGS system respectively.

The ACP Front End Cheque Image Capture and Data Entry function will provide the following functions:

- Scan the front and back of the cheque to capture the cheque image and MICR line information, (scanning of front and back of cheque to be completed in one pass)
- Generate index information for the cheque image
- Post-encoding of the MICR information by data of amount field and date which generate a data file for transmission.
- Data capture of full MICR line based on physical cheques (for contingency purposes)
- Review of images and data files for all captured images. Repairing of rejected items, missing items and items with incomplete or poor MICR line, based on cheque images.
- Authentication/time stamp of captured image and data files
- Generation of register of cheque data records for reconciliation and automatic balancing of the captured information
- Identify discrepancies and allow manual adjustment for balancing of captured information
- Generation of accounting entry record for entry into the presenting bank CBS.
- Re-capture of cheque images outside clearing cycle (e.g. re-capture due to poor quality)
- Tools for allocating and monitoring workload of data entry and balancing functions.

18. RULE 18 - TESTING, CERTIFICATION AND CHANGE CONTROL

18.1 Participant Pre-requisite

Each participant is required to perform all necessary modifications to their systems linked to the CIS at its own expense, as well as the recruitment of qualified personnel for the task. Participants shall accordingly ensure implementation and adherence to all relevant procedures as may be required, except in cases where the required equipment were initially provided by CBG, in which case their maintenance shall be the responsibility of the concerned users.

18.2 Service Level Specification

The Central Bank may from time to time specify the service levels to be provided by CIS and determine the service levels of the participants' systems, used in relation to the CIS.

18.3 Certification Requirement

Any new Participant has to fulfil the following steps prior to connecting to the CIS:
a) Undergo satisfactory Test of its systems and connectivity on trial basis
b) Receive a clean bill of health (Fit and Proper Test Certificate) from CBG following tests of its systems, equipment and Personnel for the CIS Operation
c) Sign and submit the Membership Agreement for the Provision of CBG National Payment Service.

18.4 Participants' Responsibility

Each participant has the following responsibilities:

    a). To develop their internal systems for linking to / from CIS and the maintenance, security and reliability (including back-up and contingency arrangements) of such systems at its own cost.

    b). To operate, administer and monitor CIS installations at the participants' site

    c). Day to day responsibility for operating its CIS equipment at participants' site, which include Application Server, Database Server, Controller PC, Operator PC and the interface between its own host system and CIS system.

18.5 Authority to Effect Change

No participant has the authority to make changes of any nature to the CIS systems or install / use any software or any part of the CIS systems without the prior written approval of the Central Bank.

18.6 Mandatory Reporting by Participant

Each participant is required to advise the Central Bank immediately of any event capable of affecting its ability to function as a Participant, including any planned or sudden disconnection from the network. This shall include any significant events such as matters of interface with the CIS, organizational structure, change of personnel responsible for the CIS, environmental alterations etc.

18.7 Internal Operating Guideline and Procedure

Each participant and the Central Bank shall implement their own internal guidelines and procedures, to ensure compliance with these Operating Rules. The Operational Rules shall take precedence over such guidelines in the event of conflict between the two.

18.8 Operations by Participants

Each participant shall operate the areas of CIS, in line with its control and responsibilities, as contained in the Operational Rules and any other appropriate Control document issued by CBG from time to time.

18.9 Change Control

18.9.1 CIS Changes

The Central Bank is authorized to make any changes to CIS and to issue guidelines to the effect. Thereafter, Participants shall be advised accordingly, giving reasonable notice to all participants before the changes are implemented.

The Central Bank may also provide directions for the safe and timely implementation of changes, which may include additions or amendments to the existing rules. Participants

may, where necessary, propose amendments and forward to CBG for consideration and approval, although the latter is not obliged to implement such proposals.

18.9.2 Implementation of Changes

Each participant shall ensure that its internal procedures and systems have the capability to deal effectively with new or amended guidelines, Operational Rules or any other provisions issued by CBG at all times.

18.9.3 Advice of Changes

These Operating Rules are issued by the Central Bank to all CIS Participants for effective implementation in The Gambia. Each Participant is responsible for keeping the Central Bank informed of any changes in their contact details for the purpose of up-dating all other Participants through appropriate communication channels.

19. RULE 19 - FEES AND CHARGES

The participants shall pay fees in accordance to their membership and usage of the system. Such fees and charges shall be paid in the amount and manner prescribed by CBG in a CBG Payment Systems Pricing Policy and will announce the tariff and fees information to all participants by circular.
CBG shall also apply penalty charges to individual participants in the event that the concerned participants have taken actions, which may hamper the efficiency, security or customer protection within the CIS operations. The rules for penalty charges are described in the following sub-sections.

19.1 Fees

As a general principle, CBG reserves the right to define or modify the fee categories and their tariff structure. CBG shall advise the fees tariff, and any future amendments if necessary, to all participants via appropriate mechanism.

19.2 Penalty Charges and Other Service Fees

CBG may prescribe penalty charges and other service fees for operating the system on behalf of all Participants, including the imposition of fines for violations.

19.3 Collection of Fees and Charges

Central Bank reserves the right to collect the fees and charges from participants via the RTGS system. Central Bank will advise the procedure and billing time via appropriate mechanism to all Participants.

19.4 Fees and Charges Policy

CBG shall prepare a policy on applicable 'Fees and Charges' and shall notify Participants each time there are revisions.

20. RULE 20 – EMERGENCY CONDITIONS

20.1 Authority

The Central Bank has the special authority to perform the appropriate action under the emergency conditions, including but not limited to the provisions of Rule 24 sub-section 24.6.

20.2 Request for Extension

Should there be need for an Extension of the CIS service on behalf of a Participant, the Participant must first be prepared to pay a levy or relevant penalty and must complete the following steps:
      a) Log a Call with the CBG
      b) Send a written request to the CBG with authorized signature.
The Central Bank shall exercise discretion to approve or reject the extension request. Upon granting the extension, a message is sent to alert all participants.

20.3 Session Termination

CBG may terminate a clearing session in an emergency situation. The system shall perform the following under abrupt termination:

- Stop accepting new cheques presented on same terminated session; cheques will be accepted upon opening of next schedule session.
- All pending cheques awaiting reply will be rejected from CBG with the message "session terminated".
- All cheques already replied to by the Issuing Bank will retain the same status and be scheduled for settlement at the next clearing.

20.4 Failure of Clearing Settlement

In the event that any Participant cannot fulfil its Settlement obligations, the Central Bank will inform the Participant accordingly. It is the responsibility of the Participant to provide the funding and complete the settlement on the value date.

21. RULE 21 - BUSINESS CONTINUITY

21.1 Case 1: Failing of the system at the Participant's Site

In the event of systems failure, the concerned participant shall immediately inform the System Administrator at CBG, to investigate and assist in providing an immediate resolution. This may require CBG to provide an alternate path for connecting the

participant to CIS central site, or arranging the installation of backup network equipment for the participant.

At the same time, the participant must inform CBG of the failure and the efforts being made towards resolution.

If the failure is anticipated to be protracted, the Participant must arrange personnel to carry its urgent physical cheques to the CBG Clearing House. The participant shall request to use the emergency service (**Service Bureau**) at CBG as a temporary arrangement. Under such circumstances, the CBG may avail Participants scanners and workstations at the Clearing House.

21.2 Case 2: Failing of the CIS Central Site

The CIS System administrator shall immediately inform all the participants of the failure via telephone, fax or emails. CBG will activate the CIS Backup site and restart the CIS services from the Backup site. CBG shall inform all participants when the services are restarted. The participants must then reconnect their CIS workstations to the Backup site and resume processing.

In switching the service to the Backup Site, the participants must reconcile their pending cheques and replied cheques at the Backup Site system, and if necessary, to perform re-capture of any paper cheques which are not identified in the Backup Site system.

21.3 Case 3: Failing of the CIS Workstations or Scanners

The CIS is a fully web enabled system. In the case of any CIS workstation failure, participants shall re-connect to CIS from any operational workstation with the necessary configuration and web browser. Participants shall also cater for at least one backup CIS scanner for their head office and branch.

22. RULE 22 – DISCIPLINE

22.1 Authority

The Central Bank shall have the authority to take necessary timely action against Participants to ensure the efficient operation of the CIS.

22.2 Suspension of Participant

The Central Bank may suspend or expel Participants either temporarily or permanently, if the Participant is judged to have violated the rules as follows:
- failure to meet the qualifying criteria prescribed by CBG from time to time, such as non-compliance with interface requirements for the smooth operation of CIS;
- participant is insolvent or bankrupt;
- participant's banking license is revoked;

- persistent failure to comply with these operating rules;
- any other reason deemed appropriate by the Central Bank.

22.3 Suspended Participants obligation

In the event of suspension, the concerned Participant's pending (non-replied) cheques shall be automatically rejected by the system. The suspended participant shall still be liable for settlement of all cheques which are replied by the participant for payment. The participant shall also remain liable for any other accrued and accruing obligations under the CIS Operating Rules. The Central Bank shall direct the suspended participant to surrender its rights, systems, software and any other related materials.

23. RULE 23 - DEFAULT PROCESSING

23.1 Authority

The Central Bank has the authority to suspend a defaulting Participant, as per the provisions prescribed in these operating rules or as per the relevant Banking Act in The Gambia.

23.2 Notification of Default

The Central Bank shall determine the magnitude of default and the point of notification of the Participant concerned. Thereafter, the relevant sanctions shall apply, taking into consideration the circumstances leading to default, frequency of default and the injury caused to other Participants.

23.3 Participant Obligation

All Participants obligations shall be as prescribed in these Operational Rules and any other relevant regulations.

24. RULE 24 - OBLIGATION TO LAW (MISCELLANEOUS PROVISIONS)

24.1 Central Bank of The Gambia

Notwithstanding anything to the contrary stated in the CIS rules and regulations or any of the reference documents, the Central Bank and its officers, employees and/or agents shall not be liable to the Participants or any other third party for any losses, damages or expenses incurred directly or indirectly from any of the following:

• Delay caused due to breakdown, malfunctioning or deficiency of CIS system including hardware, software, telecommunication and electrical systems.
• Partial or complete disruption or failure of CIS to provide all or any other services intended by CIS.
• Failure of the participant's own systems.
• Negligence, fraud, dishonesty, misconduct, errors or omissions on the part of Participants or its system users.

24.2 Fraud

Any loss arising due to fraud originated at the Participant's business shall be borne by the relevant Participant.

Central Bank is authorized to interrupt any transaction should it fall suspicious of money laundering or terrorism financing activities.

24.3 Force Majeure

The Central Bank or any Participant shall not be liable for any losses due to failures resulting from the genuine implementation of these Operating Rules, or any obligations arising directly or indirectly from circumstances beyond its control, including but not limited to, industrial action of any kind, government action, natural calamity, riot and/or war.

24.4 Central Bank Personnel

Nothing in these Operational Rules shall be prejudicial to the liability to the Central Bank or its employees or agents for their actions or omissions as specified by the laws of The Gambia.

24.5 Officers, employees and Agents

The provisions of Rule 24 Subsection 24.1 and 24.2 shall by extension apply to the benefit of officers, employees and agents of CBG in respect of implementation of these Operational Rules.

24.6 Emergencies

If any malfunction, breakdown, or interruption or any emergency affects CIS or its operations, transactions shall be handled in accordance with the emergency policy of the Central Bank, whilst using its discretion as may be appropriate.

24.7 Participants Act as Principals

Each participant shall be liable as the Principal in transacting its own cheques.

24.8 Assignments

No Participant shall assign all or any of its rights or obligations under these Rules, Participants agreement or any other relevant.

24.9 Dispute Resolution

The participant and the central bank agree that the RTGS database electronic records and timestamps archived by the central bank shall be regarded as the exclusive evidence of the transactions.

The Participants agree that every effort shall be made to resolve amicably by direct negotiation, any disagreement or dispute arising between them under or in connection with these Rules.

Where attempts at direct negotiation have been unsuccessful, notification of intent to dispute must be sent to the other Participant and the Overseer, setting out a full description of the matters in dispute within fourteen (14) days of such intention arising.

Pending the resolution of the dispute, the Participants will continue to perform all their obligations under these Rules.

The Chief Executive Officers of the Participants must personally or through nominees attempt to resolve the dispute amicably, on the basis that the Participants wish to retain an ongoing relationship.

If the Chief Executive Officers, or their nominees, are unable to resolve any dispute within seven (7) days of the notice or any other time frame as the Participants may agree, then either Participant may give notice to the other Participant that the matter is not resolved and that the Participant shall refer the dispute to arbitration before a single arbitrator in accordance with the Arbitration Act of the Laws of Gambia or any statutory modification or re-enactment thereof for the time being in force. The decision of such arbitrator shall be final and binding on the Participants.

24.10 Governing Laws

These Operating Rules, Participants' agreement and any other regulations issued by CBG shall be governed by the appropriate Laws of The Gambia.

25. RULE 24 – SUPPORT SERVICES

25.1 Central Bank Payment Systems Unit Help-Desk

Should there be any changes, either at CBG or Participant level, the Central Bank will advise Participants regarding the new contact details of the Payment Systems Unit Help-Desk via email, circulars or like medium, or publish them on its web-site.

25.2 CBG Contact Details

The CBG contact details, for matters relating to CIS operations, are as provided in Appendix V, revised and advised by CBG from time to time.

25.3 Participants' Contact Details

Refer to Appendix IV and V (to be updated regularly by CBG)

26. APPENDICES

- **Appendix I -   Glossary/Definition of Terms**
- **Appendix II –   Core Banking System Interfaces**
- **Appendix III –   Inward Clearing List (ICL) File Specification**
- **Appendix IV -   List of Participants Bank Numbers (Bank Code)**
- **Appendix V-   CBG Contact Details**
- . **Appendix VI: Types of Instruments Supported**

26.1 Appendix I – Glossary

Ref	Term	Definition
1.	CIS Payment System	Cheque Imaging System (CIS) is part of the National Payment System being developed by the Central Bank in The Gambia. The CIS is an electronic platform through which Participants (Direct and Indirect) exchange cheque payments using electronic image and data records, instead of physical paper cheques. The CIS performs automatic clearing of cheque image and data amongst the commercial banks over scheduled clearing sessions on each business day.
2.	Access Control List	A security control to define the list of allowed users privileges which are authorized by CBG system administrator for granting to the head office and branch users of a participant. Users or participants are not allowed to access any function not authorized or open to them.
3.	Administrator/System Administrator	A user role established in the CIS with responsibility to perform all daily maintenance of system parameters, participant /user/account information, business rules in order to suit operational requirements of the CIS participants.
4.	Presenting Bank	The participant bank that receives a cheque and Initiate its clearing process on behalf of the customer. The Presenting (Initiating) bank presents the cheque through the Central Bank Cheque Imaging System and collects funds from the Issuing Bank (see 'Issuing Bank' below).
5.	Business Calendar	A calendar of operating and non-operating days holidays of a payment system.
6.	Business Hour Timetable	The schedule of various clearing related activities to be conducted as part of operations of a system on a business day.

7.	Cancellation period	The number of working days, from the presentation date, during which the remitting participant may cancel the operation.
8.	Capture	Cheque scanning process.
9.	Clearing Account	An account maintained by the CIS System for each participant in which debit or credit instructions are posted as and when received and validated by the system to arrive at the Net clearing balance.
10.	Clearing Balance	A net position of payment instructions drawn by or drawn on a member on or by other members, accumulated up to that point of time during a business day.
11.	Clearing Cycle	Refer to Rule 4 Section 4.3
12.	Clearing House	This refers to the CBG organized Clearing process at its offices, where banks participate in clearing and settlement of cheques, ATM and various Government transactions in The Gambia.
13.	Clearing Session	A time-bound session on which cheques due for clearing are presented and replied between the presenting (initiating) participant and the Issuing (receiving or paying) participant bank.
14.	Clearing system	A set of procedures whereby financial institutions present and exchange data and/or documents relating to funds or transfers to other financial institutions at a single location (clearing house).
15.	Cheque Truncation	Electronic scanning and transferring of cheque images and data for clearing, which replaces the physical movement of paper-cheques between the banks and clearing houses. Subsequently the paper-cheques shall be truncated at a designated point after the cheque images and data have been accepted for processing.

16.	Clearing/clearance	The process of transmitting, reconciling and, in some cases, confirming payment orders prior to settlement, including the netting of payments for calculation of final positions for settlement.
17.	Commercial Banks	The banks operating in The Gambia, licensed by the CBG to carry on the normal banking business subject to the conditions of licensing.
18.	Compressed file (triplicate)	Triplicate of files (.ENV .CAT and .PAK) compressed in a unique file.
19.	Customer	A private person or an institution, on whose behalf (ordering customer) or in whose account (destination customer), a payment (debit or credit) is effected.
20.	Daily settlement	Completion of settlement on the day of value of all payments accepted for settlement.
21.	Debit Limit/Debit Cap	The Maximum multilateral and/or bilateral balances authorized between participats. It limits the participant's net debit position at any time of an operating day in the CIS, which may be predetermined by CBG from time to time.
22.	Debit Transfer	An instruction for debiting the designated payer's account for the purpose of placing funds at the disposal of the issuer of instruction. While the instruction moves from the bank of the issuer/originator of the instruction, funds described therein move from the bank of the payer to the bank of issuer/originator of instruction.
23.	Decryption	The use of cryptographic algorithms to decode cipher text data into clear text which was earlier encrypted to prevent unauthorized observation. (See also encryption)

24.	Default	Failure to complete a funds transfer according to its terms for reasons that are not technical or temporary, usually as a result of bankruptcy. Default is usually distinguished from a "failed transaction".
25.	Deletion	A mechanism whereby some or all transfers to/from a defaulting participant are excluded from the settlement process. In a netting scheme, either participants' bilateral and/or multilateral net positions are recalculated.
26	Differential image file	A file containing a set of generated images during a given time range.
27	Doubles	Two cheques that pass together in the same time in the scanner.
28.	Drawer Customer	This is the issuer of the cheque which has been presented into CIS for clearing by a participant on behalf of the beneficiary. The cheque is subsequently drawn on the drawer customer's bank account to request transfer of funds for payment of the cheque value to the drawee.
29.	Duplication	Two scanned or presented documents having the same identifier (MICR codeline).
30.	Encryption	Mathematical process that transforms an original message into an unusable string of characters seemingly random, but is actually fulfils precise mathematical rules. It involves the use of cryptographic algorithms to encode clear text data (plaintext) into cipher text to prevent unauthorized observation. (see also decryption).
31	Endorsement	Text automatically printed by the scanner on the paper instrument reverse side.
32.	Failure of settlement	An event of net settlement CIS transaction which cannot be settled in the RTGS for want of adequate funds in one or more of the participant's settlement accounts in the RTGS.

33.	Field	A data element(s) for which the identification, description and value representation has been predefined. Each data element constitutes an indivisible unit. Where a field consists of more than one data element, each forms a subfield. Fields may be: . Fixed length or variable length . Mandatory or optional . Restricted in the characters that may be used. A field can appear only once in a message, unless the rules specify otherwise. Some fields consist of several subfields
34.	Final	Irrevocable and unconditional.
35.	Final settlement	Settlement which is irrevocable and unconditional. The discharge of an obligation by a transfer of funds that have become irrevocable and unconditional.
36.	Finality	Settlements in payment systems which are both unconditional and irrevocable are designated as final or conclusive.
37.	Financial liability	Any liability that is a legal obligation to deliver cash or another financial instrument to another enterprise or to exchange financial instruments with another enterprise under conditions that are potentially unfavorable.
38	General Clearing Summary Statement	Daily balance statement for the exclusive usage of the Central Bank. For every participating institution, it states for each payment instrument the number and total amount of received transactions and remitted transactions. The statement notifies also the net balance for each participating institution.
39.	Intraday liquidity Facility (ILF)	Funds that can be accessed during the business day, usually to enable financial institutions to make payments in real time.

40.	Inward Clearing	Inward clearing for a bank, represents the cheques forwarded by various Banks of First Deposit (Presenting Bank), drawn on it for payment and cheques which were presented by it as Presenting Bank but have been returned by System or rejected by Issuing Bank.
41	JPEG format	Image compression standard format.
42.	Key	A unique series of digits used in combination with a cryptographic algorithm.
43.	Key length	The number of bits comprising an encryption Key.
44.	Liability	An obligation of the enterprise arising from past events, the settlement of which is expected to result in an outflow of funds (resources) embodying economic benefits.
45.	Liquidity	State of availability of funds or the ability to raise such funds towards the settlement of an obligation. The sufficiency of funds in the settlement account of the participant to meet all obligations originating from the CIS system.
46.	Liquidity risk	The risk that a counter party (or participant in a settlement system) will not settle an obligation in full when due. Liquidity risk does not imply that a counter party or participant is insolvent as the situation of illiquidity may be temporal.
47.	MICR	MICR (Magnetic Ink Character Recognition), as defined by the American National Standards Institute (ANSI), is a technology used to verify the legitimacy or originality of paper documents, especially cheque. Special ink, which is sensitive to magnetic fields, is used in the printing of certain characters on the original documents. Information can be encoded in the magnetic characters. The use of MICR can enhance security against forged or counterfeit documents. If a document has been forged - for example, a counterfeit cheque produced using a colour photocopying machine, the magnetic-ink line will either not respond to magnetic fields, or will produce an incorrect code when scanned using a device designed to recover the information in the magnetic characters.

48.	Membership	Membership is a process whereby a prospective participant of the clearing and settlement system is evaluated on application based on predetermined eligibility criteria and granted access to such a system if qualified. Membership means being subjected to compliance with the discipline prescribed in these Operational Rules.
49.	National Payment System	Payment System existing and being developed / established in The Gambia by the Central Bank. (Please also see Payment System)
50.	Net Clearing Position (NCP)	A participant's net credit or net debit position in the CIS settlement system. It is the difference between the claims for and against the participant. If the difference is positive, the participant is in a net credit position; if the difference is negative, the participant is in a net debit position. The net credit or net debit position at settlement time is called the net settlement position. These net positions may be calculated on a bilateral or multilateral basis (see also net settlement, net settlement system)
51.	Net settlement	The settlement of a number of obligations or transfers between or among counterparties on a net basis. See also Netting.
52.	Netting	An arrangement for the setting off of mutual positions or obligations between business partners or participants in the payment system. Netting reduces a large number of individual positions or liabilities to a smaller number of positions or liabilities. Netting can take different forms; these claims are legally enforceable to a varying extent in case of default by a participant (see also multilateral netting).
53.	Obligation	A duty imposed by contract or law.
54.	Outward Clearing	Outward clearing for a bank, represents the cheques forwarded by it as Presenting Bank to various Issuing Banks for payment and cheques which were presented by other banks as Presenting Banks on it but have been returned by System or rejected by it.

55.	Participant	A party or institution that is regularly involved in handling cheque payments, and has secured membership or authorization of the Central Bank to participate in the daily cheque clearing and settlement activities operated by the Central Bank for the National Payment System. (See also RULE 2.1)
56.	Issuing Bank	The participant bank which Receives cheques originally issued to its customers, being presented from the Presenting Bank through CIS for settlement. The Issuing Bank is obliged to receive these cheques as issued by their customers and to perform clearing authorization, and settlement if customer has sufficient funds in their account.
57	Paper jam	Blockage of a cheque or a bill of exchange in the scanner during scanning.
58.	Payee	The beneficiary party of a cheque as identified in the favour of payment information on the cheque of which the cheque issuer is liable to pay the cheque value amount.
59.	Payer	The customer issuing a cheque for payment of its value, upon the cheque being presented and drawn on the customer's account.
60.	Payment message/instruction/order	An order or message to transfer funds (in the form of a monetary claim on a party) to the account of the beneficiary. The order may relate either to a credit transfer or to a debit transfer.
61.	Payment system	A payment system consists of a set of instruments, banking procedures and, typically, inter-bank funds transfer systems between counterparties.
62.	Positive Pay Cheques	These are usually cheques which do not require detailed technical or financial scrutiny since these have been issued through or by Issuing Bank on its own behalf (e.g. Bankers' cheques, payment order) or where prior arrangements of funds have been made for payment.

63.	Post Dated Cheque	It is a cheque bearing a future date, which cannot be valued until that date is reached.
58.	Protocol	Procedures for the interchange of electronic messages between communicating devices.
59.	Queuing	A risk management arrangement whereby transfer orders are held pending by the originator/deliverer or by the system until sufficient cover is available in the originator's/deliverer's clearing account or under the limits set against the payer; in some cases, cover may include unused credit lines or available collateral. See also Caps.
60.	Receiver	The participant receiving a message as identified by its registered address in the header of the message.
61.	Repurchase agreement or REPO	An agreement with a commitment by the seller to buy a security back from the purchaser at a specified price at a designated future date.
62.	Request	Message sent to CIS to receive answer on status of the file/batch/individual transaction, etc.
63.	RTGS	Real Time Gross Settlement System. This is the settlement system being used for settlement of any interbank payment on real time and gross level basis, as part of the National Payment System in The Gambia.
64.	Security	In relation to a Payment System, it involves protection from unauthorized physical or logical access to the system's live or stored data and data in transmission.
65.	Settlement Agent	A participant in the Payment System which undertakes to settle the obligations of another participant through its own settlement account in a Payment System.

66.	Server	A computer with much larger storage space which provides services through a network to other computers.
67.	Settlement	The actual fulfillment of the clearing obligations, i.e. the transfer from the banks with net debit positions to the banks with net credit positions to cancel out outstanding obligations against each other. This transfer is carried out via a central counterparty.
68.	Settlement account	An account held by a direct participant in the CBG's RTGS system for the purpose of processing payments.
69.	Settlement date	The date on which the parties to the funds transfer request agree that settlement is to take place. The intended date is sometimes referred to as the contractual settlement date.
70.	Settlement risk	A general term used to designate the risk that settlement in a transfer system will not take place as expected. This risk may comprise both credit and liquidity risks (see also credit risk, liquidity risk,
71.	Settlement system	A system used to facilitate the settlement of transfers of funds or financial instruments.
72.	Systemic risk	The risk that the failure of one participant in a transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations (including settlement obligations in a transfer system) when due. Such a failure may cause significant liquidity or credit problems and, as a result, might threaten the stability of financial markets.
73.	Transaction Reference Number	This field specifies the reference assigned by the Sender to unambiguously identify the message.

74.	Transfer	Operationally, the sending (or movement) of funds or securities or of a right relating to funds or securities from one party to another by
		(i) conveyance of physical instruments/money;
		(ii) (ii) accounting entries on the books of a financial intermediary;
		(iii) or accounting entries processed through a funds and/or securities transfer system.
		The act of transfer affects the legal rights of the transferor, transferee and possibly third parties in relation to the money balance, security or other financial instrument being transferred.
75.	Value Date	Day on which a payment is due to be credited to the Payee customer of a cheque payment instruction.
76	XML	Extensive Markup Language, which is a standard for describing data information by computer application software in a way which will facilitate exchange or sharing of information between different computer systems. It is a formal recommendation from the World Wide Web Consortium (W3C), and is similar to the HTML language of Web pages. Like HTML. XML contains markup symbols to describe the contents of data information.

26.2 Appendix II - Core Banking System Interfaces

26.2.1 Checkout

The system shall execute the cheque out cycle as outlined in the diagram below

Outgoing clearing process

Presenting Branch

Cheques and Bank Drafts → **Scanner** LS515

Barberousse - Capture

- Scanning both sides of images values
- Reading the MICR tracks
- Encrypting images
- Input of addtional information of cheque or bank drafts (amount, issuing date, etc...)
- Validation of scanned values
- Generation of image and idex files (.CAT/.PAK)
- Generation of data files

CBA Data records

Barberousse - Générateur des clés

Images (.CAT/.PAK) and data files

Presenting Bank

Hannibal -Autocollecte

Collect secured image and data files

Hannibal - ADT

- Control of the validity of the received files (images, index and data)
- Authentication of images files
- Cross matching .CAT (index) and .PAK files
- Reconciliation between images and data
- Control CBA data records
- Generation of interbank remittances to clearing center
- Generation of intrabank remittances to branches
- Calculation of provisional clearing balance

CBA Data records

Barberousse - Générateur des clés

Images and Data files

Hannibal - Poste Adhérent

- Authentification of images files
- Cross matching .CAT (index) and .PAK files
- Logical and syntax control of data files
- Rconciliation between images and data
- Control, singnature and encryption of images
- Deposit and encryption of images and data files
- Displaying of errors and reject invalid files
- Displaying Outgoing remittances

MAIL BOX : Electronic data remittances and images files sorted by currency, center and value type

Clearing House

Hannibal - Autocollecte

Collect encrypted Remittances from Presenting Bank

26.2.2 Check-In

The system shall execute the cheque-in cycle as outlined in the diagram below.

Incoming clearing process

Clearing House

Hannibal - Compensation

- Image Authentication
- Cross matching between images and index files
- Control of the received files (syntax and logical controls)
- Legal controls
- Reconciliation between images and data records
- Reject invalid files and stop invalid records
- Calculation of clearing balances ant net positions
- Setting settlement shedules
- Management of Debit limits
- Sorting, generation and encryption of images and data files by receiving bank
- Generation of interface files to RTGS, ATM / POS systems

Hannibal-Serveur Web

- Archiving generated files
-Viewing images and data archived
- Management of authorisations and access rights
-Displaying of the search results

Desk Service

Hannibal-Poste de Secours
- Images Authentication
- Logical and syntax control of data files
- Deposit of images and data files
- Recovery received files
- Displaying received remittances and clearing results

Barberousse-Présentation
- Loading data files of scanned images
- Entrying operations
- Loading clearing return files
- Rejecting operations

Barberousse-Capture

Sending return files (images, data, net positions…)

Hannibal - Autocollecte

Sending return files (images, data, net positions…)

Receiving Bank

Hannibal - Poste Adhérent

- Consulting received files
- Recovery received files
- Displaying Clearing results

Hannibal - ADT

- Control Clearing house result
- reconciliation between images and data received from ACP
- Sorting remittances by receiving branch
- Calculation of provisional clearing balance
- Displaying Clearing results

Access to Hannibal-Serveur Web

Barberousse Keys Generator

Hannibal - Autocollecte

Sending Return files to Branches

Receiving Branch

Barberousse – GIP Vice de Forme

- Loading received files
- Consultation of images and data
- Interfacing with signature verification system
- Treatment and generation of rejection operations
- Consultation of archived images and data by acces to Hannibal-Serveur Web
- Report received images

Barberousse Keys Generator

26.3 Appendix III – Inward Clearing List (ICL) File Specification

Validation and Reconciliation

The ACP host will verify and authenticate all input from participants according to the security requirements of the system and the overall NCB infrastructural security requirements.

The ACP host will validate and reconcile the input data by:
- Transmission
- Batch
- Item

Validation checks performed will include the following:
- Value of transmission and batch is within maximum and minimum range
- Valid sender id
- Valid currency
- Valid amounts
- Valid date
- Batch totals correct
- Maximum cheque value not exceeded
- Mandatory fields present
- Correct sequence of fields
- Correct content
- Validation of conditional fields

The ACP Host system must be able to reconcile the record counts of the outward and inward clearing files.
The process will validate that the file format adheres to specification. All mandatory fields at file level will be validated. All control fields will be matched with the record details.

Checking type	Rejection motive
Coherence control	Duplicate remittance
	Control records (number of items, total amount) inconsistent with the detailed records
	Inconsistency of operation codes in Header, detailed records and control records
	Non-existing or invalid operation code
	Non-existing or invalid locality
Format control	Empty mandatory field in remittance header or control record
	Wrong formats in file header, detailed records and control records
	Wrong type of format
	Wrong justification on alphanumeric and / or alphabetic fields
	Field filled with invalid predefined value

Participants control	Presenting participant is suspended
	Presenting participant is excluded
	Wrong direct participant identification
	Wrong indirect participant identification
Amount Control	Transaction amount above the fixed limit

The host system should also generate an audit trail and the required reconciliation records.

Inward cheques image file

Inward cheque image files are forwarded to the issuing bank at each clearing session.

The system will support multiple deliveries of inward cheque images during the clearing session to the participants

Each participant bank is able to receive the following types of files at the ACP Front End system from the ACP Host:
- Inward cheque images and MICR-encoded information for verification at the issuing bank.
- Inward return cheques with reason codes
- Reports and reconciliation totals.

Inward Return Cheques

The system will process return cheques which are presented but are rejected by the issuing bank.

The system will allow up to three configurable two digit rejection codes on each return cheque.

The ACP Front End system will process return cheque items as follows:
- Mark the status and rejection reason code on the corresponding inward cheque record
- Reverse the accounting entry, if necessary, in the bank's Core Banking System
- Retain the return cheque image for a configurable period, for the purpose of audit trail or re-submission (see below)
- Generate a return item for transmission to the clearing centre.

Return items will be batched and transmitted to the clearing centre within the time period defined in the clearing cycle.

Inward return files, reports and returned cheque images should be ready for participant banks to collect them at a pre-defined time (e.g. 14:15 hours). A reasonable buffer should be reserved for post-processing activities.

Under some circumstances, the presenting bank will require to re-transmit a return cheque to the Clearing House to retry clearing e.g. the issuing bank notifies that the payee account is now in funds.

The system must allow the presenting bank to**:**
- Retrieve the return cheque item and mark it for re-transmission to the ACP Host system;
- Generate a new index such that the item will not be rejected as a duplicate submission. The new index should link to the previous index for auditing purpose;
- Define a limit on the maximum number of times (e.g. three times) for re-submitting return cheques.

Once the return cheque is re-submitted with a new index, the ACP Host system should process it in the same manner as normal outward clearing cheque.

26.4 Appendix IV – List of Participants' Details

Participant Name	SWIFT BIC Code	CBG CBA T24 Account Number
Central Bank of The Gambia	CBGAGMGM	Not Applicable
Standard Chartered Bank	SCBLGMGM	5101000012
Trust Bank	TBLTGMGM	5101000029
Arab-Gambian Islamic Bank	AGIXGMGM	5101000036
First International Bank	FIBLGMGM	5101000043
Guaranty Trust Bank	GTBGGMGM	5101000050
International Commercial Bank	ICBGGMGS	5101000067
Access Bank	ACGAGMGF	5101000098
Eco Bank	ECOCGMGM	5101000108
BSIC Bank	BSAHGMGM	5101000115
Prime Bank	PRBGGMGG	5101000139
Bank PHB	ITBCGMGM	5101000146
Skye Bank	SKYEGMGM	5101000153
Zenith Bank	ZEIBGMGM	5101000160

Institution name and code	Branch code	Branch name	REGION
001 STANDARD CHARTERED BANK	101	BANJUL	BANJUL
	201	SEREKUNDA	KANIFING MUNICIPALITY
	202	KAIRABA AVENUE	KANIFING MUNICIPALITY
	203	SENEGAMBIA	KANIFING MUNICIPALITY
	701	BASSE	UPPER RIVER REGION
002 TRUST BANK LTD	101	BANJUL	BANJUL
	201	WESTFIELD	KANIFING MUNICIPALITY
	202	BAKAU	KANIFING MUNICIPALITY
	203	BAKOTEH	KANIFING MUNICIPALITY
	204	LATRIKUNDA SABIJI	KANIFING MUNICIPALITY
	205	SERREKUNDA MARKET	SERREKUNDA
	206	BUNDUNG	BUNDUNG
	301	BRIKAMA	WESTERN REGION
	302	YUNDUM	WESTERN REGION
	401	SOMA	LOWER RIVER REGION
	501	FARAFENNI	NORTH BANK REGION
	502	BARRA	NORTH BANK REGION
	701	BASSE	UPPER RIVER REGION
003 AGIB	101	BANJUL	BANJUL
	201	WESTFIELD	KANIFING MUNICIPALITY
	202	SENEGAMBIA	KANIFING MUNICIPALITY
	301	BRIKAMA	WESTERN REGION
	701	BASSE	UPPER RIVER REGION
004	101	BANJUL	BANJUL

F I BANK	201	SEREKUNDA	KANIFING MUNICIPALITY
	202	KAIRABA AVENUE	KAIRABA AVENUE
	203	LATRIKUNDA SABIJI	KANIFING MUNICIPALITY
	204	BAKAU NEWTOWN	BAKAU NEWTOWN
	301	BRIKAMA	WESTERN REGION
	302	KANILAI	KANILAI
	701	BASSE	UPPER RIVER REGION
005 **GUARANTY TRUST BANK**	101	BANJUL	BANJUL
	102	BANJUL MARKET	BANJUL
	201	KAIRABA AVENUE	KANIFING MUNICIPALITY
	202	SEREKUNDA	KANIFING MUNICIPALITY
	203	LATRIKUNDA SABIJI	KANIFING MUNICIPALITY
	204	BUNDUNG	KANIFING MUNICIPALITY
	205	BAMBO	KANIFING MUNICIPALITY
	206	SENEGAMBIA	KANIFING MUNIPALITY
	207	BAKAU MARKET	KANIFING MUNICIPALITY
	208	OLD JESHWANG	KANIFING MUNICIPALITY
	209	JIMPEX	KANIFING MUNICIPALITY
	301	BRIKAMA	WESTERN REGION
	302	BRUSUBI	WESTERN REGION
	501	FARAFENNI	NORTH BANK REGION
	701	BASSE	UPPER RIVER REGION
006 **INTERNATIONAL COMMERCIAL BANK**	101	BANJUL	BANJUL
	201	SEREKUNDA	KANIFING MUNICIPALITY
	202	KAIRABA AVENUE	KANIFING MUNICIPALITY
	203	LATRIKUNDA SABIJI	KANIFING MUNICIPALITY

007 **ACCESS BANK**	101	BANJUL	BANJUL
	201	SEREKUNDA	KANIFING MUNICIPALITY
	202	KAIRABA AVENUE	KANIFING MUNICIPALITY
	203	SENEGAMBIA	KANIFING MUNICIPALITY
	301	BRUSUBI	WESTERN REGION
	501	BARRA	NORTH BANK REGION
	701	BASSE	UPPER RIVER REGION
008 **ECOBANK**	101	BANJUL	BANJUL
	201	KAIRABA AVENUE	KAIRABA AVENUE
	202	KANIFING	KANIFING MUNICIPALITY
	203	BAKAU	BAKAU
	501	FARAFENNI	FARAFENNI
009 **B S I C**	101	BANJUL	BANJUL
	201	KAIRABA AVENUE	KANIFING MUNICIPALITY
	202	FAJARA	KANIFING MUNICIPALITY
011 **PRIME BANK**	201	KAIRABA AVENUE	KANIFING MUNICIPALITY
012 **BANK PHB**	101	BANJUL	BANJUL
	201	SEREKUNDA	KANIFING MUNICIPALITY
	202	KAIRABA AVENUE	KANIFING MUNICIPALITY
	203	BAKAU	KANIFING MUNICIPALITY
	204	JESHWANG	KANIFING MUNICIPALITY

013 **SKYE BANK**	**201**	KAIRABA AVENUE	KANIFING MUNICIPALITY
014 **ZENITH BANK**	**101**	BANJUL BRANCH	BANJUL
	201	KAIRABA AVENUE	KANIFING MUNICIPALITY
901 **CENTRAL BANK** **OF THE GAMBIA**	**101**	BANJUL BRANCH	BANJUL

26.5 Appendix V – CBG Contact Details

Name	Designation	Contact Details
Mr. William Eunson	Director, Banking Department	Tel (Office) 4229023 Email: weunson@cbg.gm
Mrs. Saffie Secka	Head, ACP/ACH Unit	Tel (Office) 4223171 Email: ssecka@cbg.gm
Mr. Ahmed S. B. Bojang Ms. Haddy Ceesay	Other ACP/ACH Officers	Tel (Office) 4229826
Help Desk		Tel (Office) 4226614 Fax: 4226969 Email: acp-ach-hotline@cbg.gm

26.6 : Appendix VI: Types of instruments supported

The system supports all electronic or paper instruments in general use in The Gambia and beyond. These include the following paper instruments (referred to as 'cheques' in these Operational Rules unless otherwise specified):

- Commercial and personal cheques
- Bank cheques
- Bank Drafts
- Banker's payments
- Dividend Warrants
- Interest Warrants
- Debit notes
- Payment Orders (Central Bank issued)
- High-priority special clearing cheques (not mandatory)
- Post-dated cheques (not mandatory)
- Direct debit