2.6.2 Specification of processes

As a result of system design (Phase I), the following documents are attached.

G-1 and G-2 of Appendix are referred to understand how to view the diagrams and tables.

Table 2.6.2-1: List of Processes

No.	App. Code	Process Name	Process Outline
1	V011	PIB Verification I result registration	Register the result of PIB verification I including any noncompliances found and print out Instruction Note when required.
2	V012	PIB Verification I result update	Update any mis-typings or necessary corrections during registration of PIB verification I.
3	V013	PIB Verification I result deletion	Delete any data that has been registered by mistake in PIB verification I.
4	V014	PIB Verification I result retrieval	Retrieve the registered PIB verification result of PIB verification I.
5	V021	PIB Verification II result registration	Register the Regional Office Code, NPWP and the submission date of NHVDI-I to verifier II, then outputs NHVDI-II. This process is done by verifier from Verification I, at the end of Verification I every certain time. NHVDI-II is filled in with calculations retrieved from Verification I Result DB.
6	V022	PIB Verification II result update	It is not only used for correcting mis-typings and necessary corrections, but also used to register the result of PIB Verification II.
7	V023	PIB Verification II result deletion	Delete any data that has been registered by mistake in PIB verification II.
8	V024	PIB Verification II result retrieval	Retrieve the registered PIB verification result of PIB verification II.
9	V034	PIB Verification result quarterly report A1 retrieval	Retrieve only Attachment I of PIB verification result quarterly report in specified Regional Office, sorted by importer.
10	V041	Audit result registration	Register only the Assignment Letter Number.
11	V042	Audit result update	Update any additional data and/or mis-typings during registration in Audit Result.
12	V043	Audit result deletion	Delete any data that has been registered by mistake in registrate Audit Result.
13	V044	Audit result retrieval	Retrieve the registered Audit result and print out Company Performance and Audit Report when required.

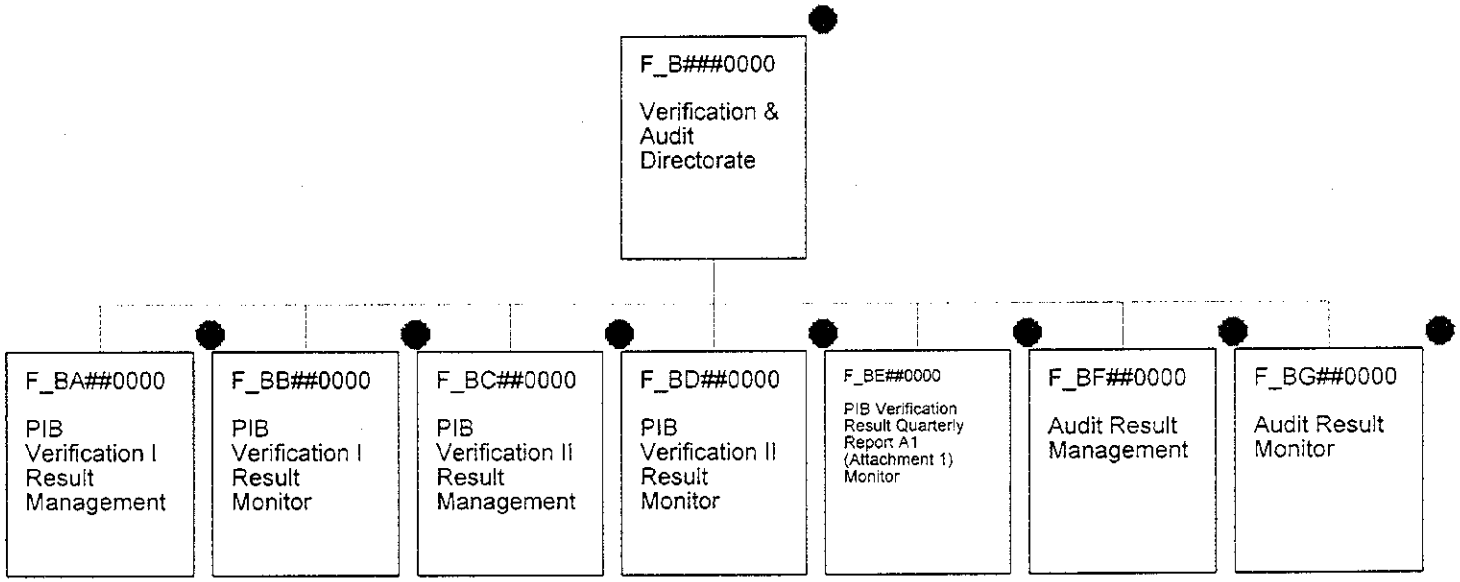

Figure 2.6.2-1: Process Structure (1/3)

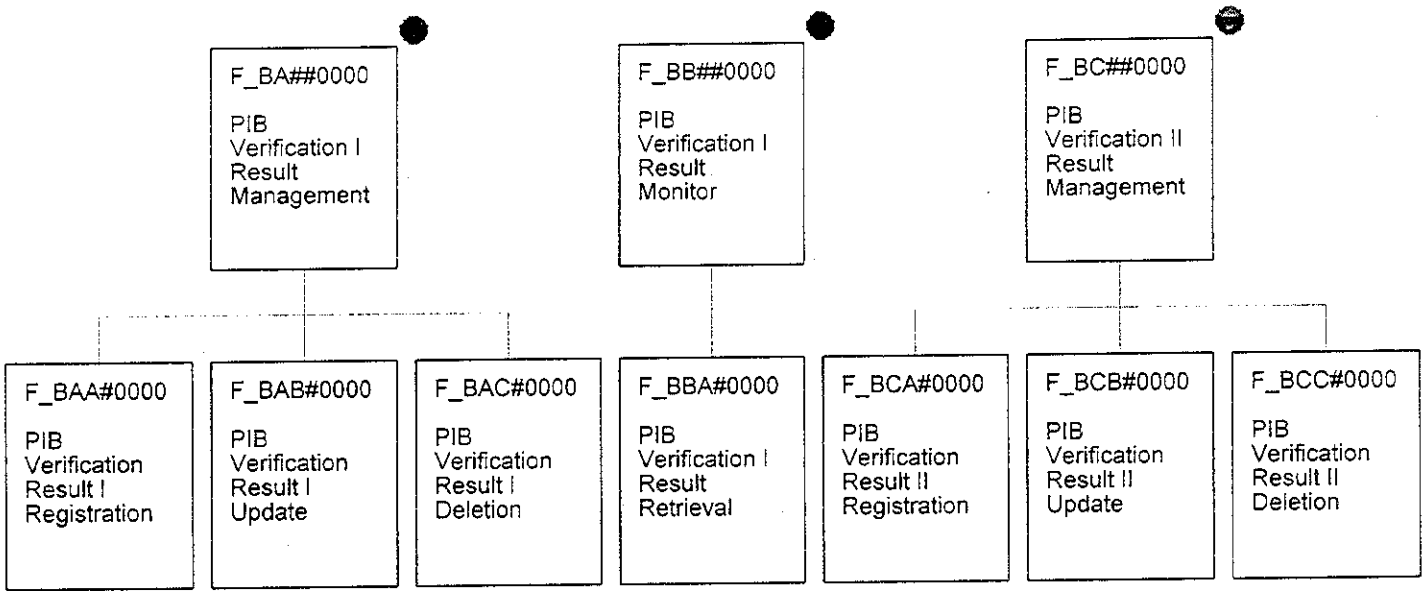

Figure 2.6.2-1: Process Structure (2/3)

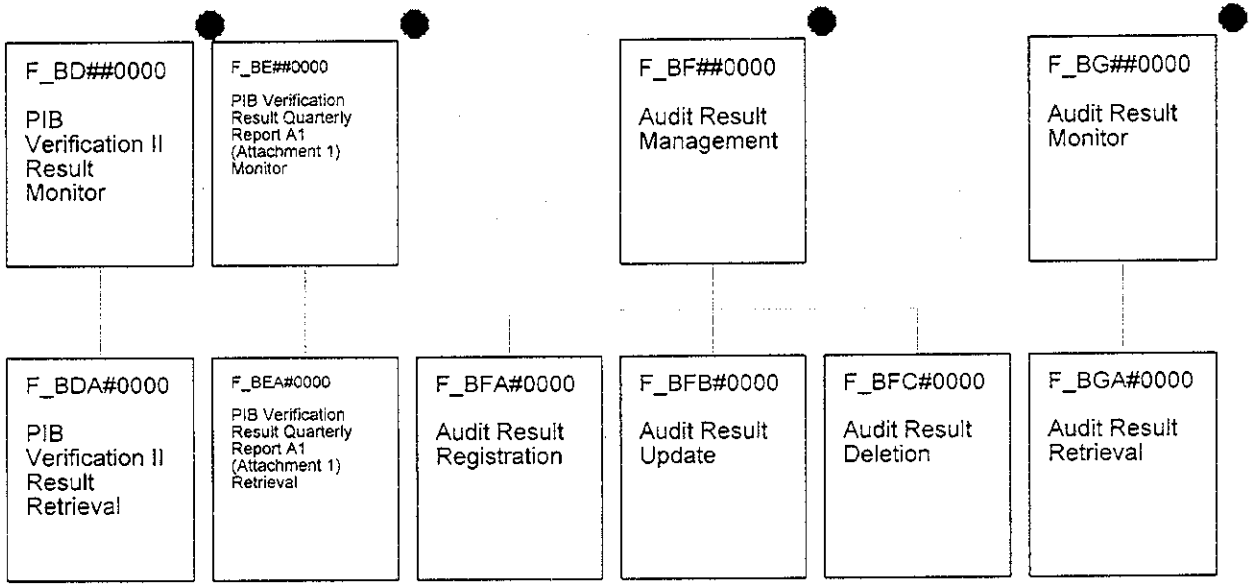

Figure 2.6.2-1: Process Structure (3/3)

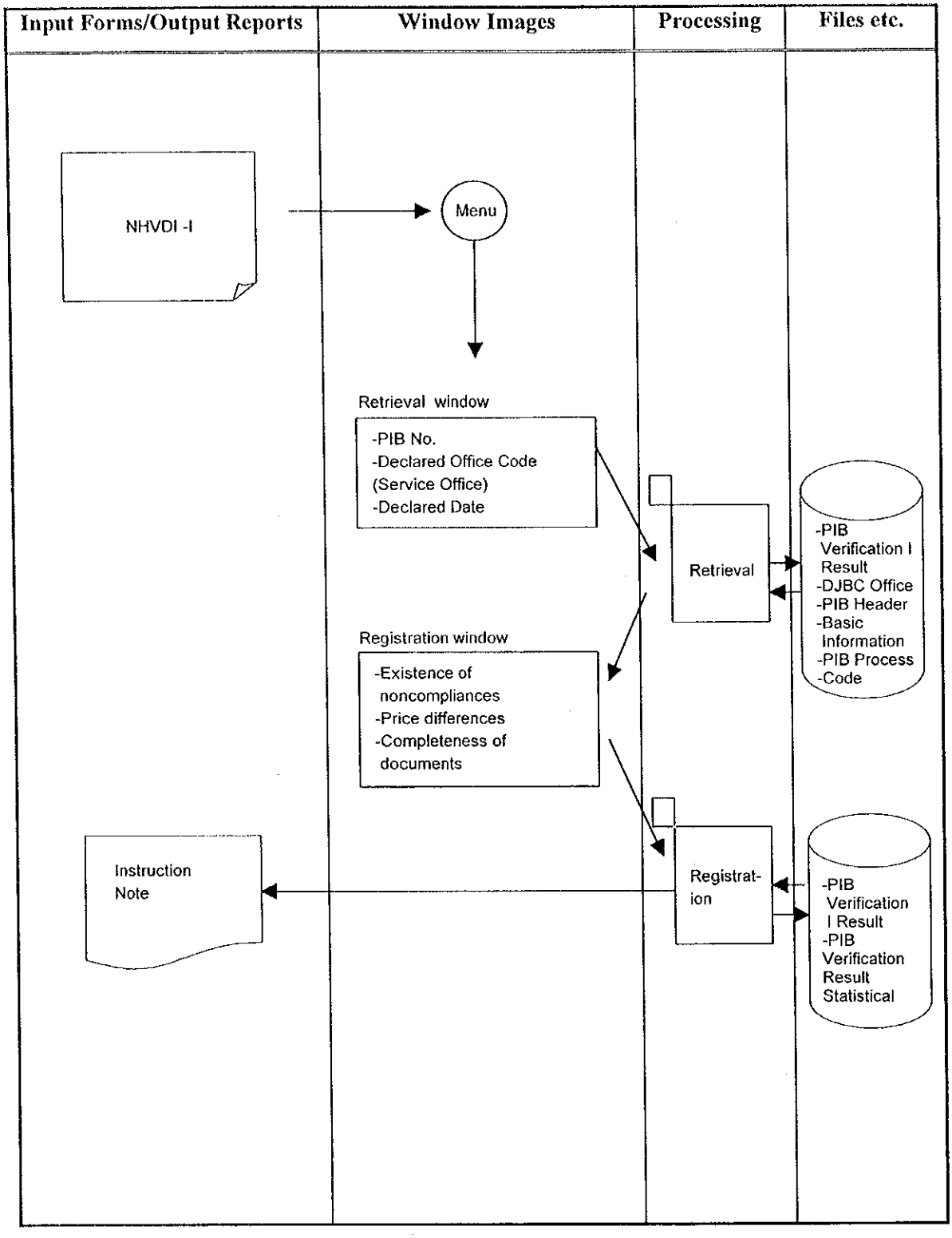

Figure 2.6.2-2: Process Diagram (PIB Verification I Result registration)

Table 2.6.2-2: Process Summary (PIB Verification I Result registration)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ PIB declaration number ▫ Declared Office Code (Service Office) ▫ Declared Date	CRT (Client)	• Registration Window ▫ Name ▫ Address ▫ NPWP ▫ Part of PIB	CRT (Client)	• PIB Verification I Result • PIB Header • Basic Information • DJBC Office • PIB Process • Code	(A) Processing Unit Processed on every PIB. (B) Processing Procedure (1) Retrieval of PIB Header information When PIB declaration number, Declared Office Code, Declared Date are inputted, the PIB Header information will be retrieved. Basic Information will then be retrieved based on the NPWP number (inc. name, address, and so on). (2) Registration of PIB Verification I Result information When verification result data is inputted into PIB Verification I Result registration window, check and register the information in PIB Verification I Result and PIB Verification Result Statistical. Output the Instruction Note if necessary.	• Directorate must be Verification & Audit (inc. Regional Office).	• Date is necessary for the primary key because PIB Number in Service Offices resets the number everyday.
2	• Registration Window ▫ Existence of noncompliances ▫ Price differences ▫ Completeness of documents	CRT (Client)	• Instruction Note ▫ Additional payment ▫ Refund	Printer (Client)	• PIB Verification I Result • PIB Verification Result Statistical			

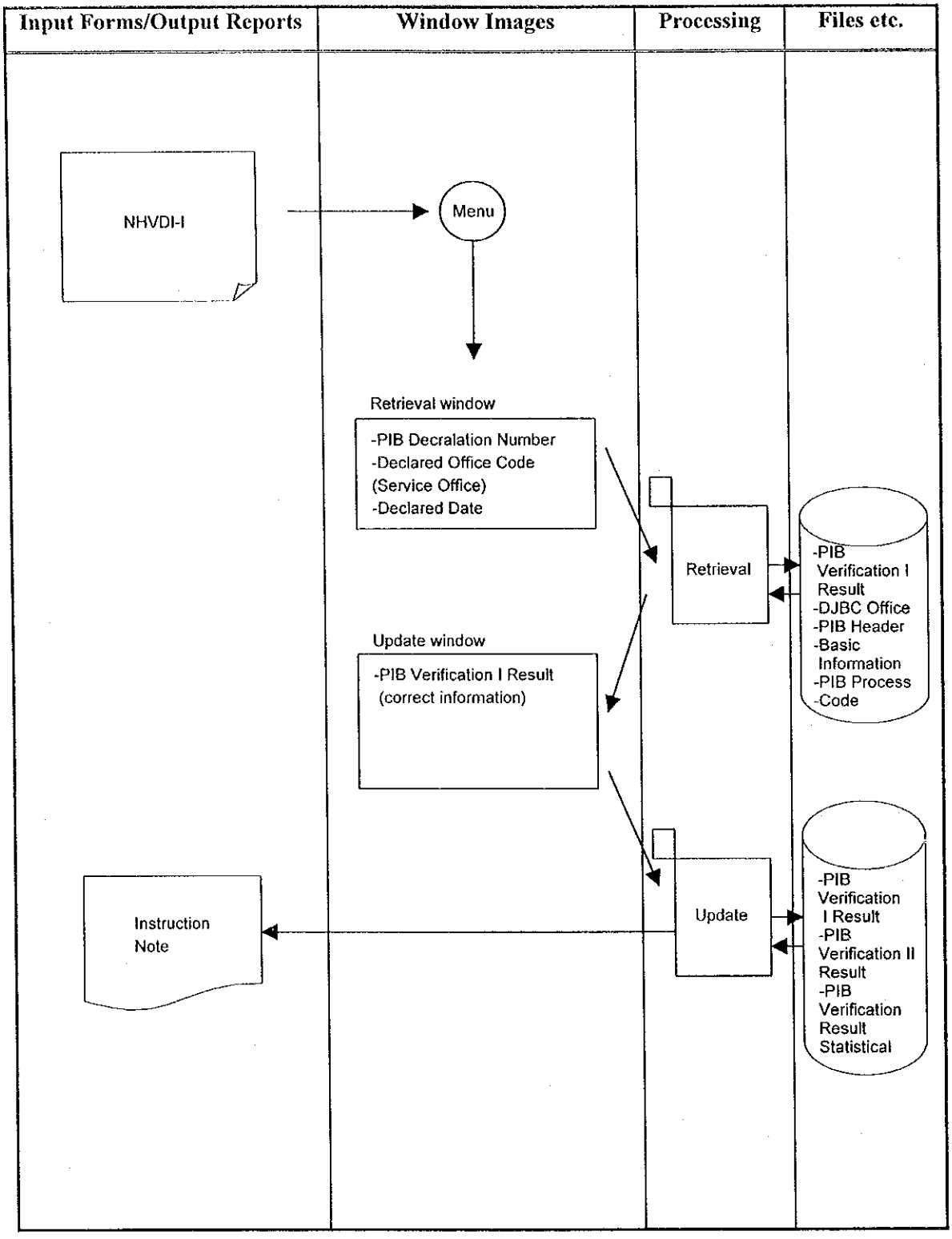

Figure 2.6.2-3: Process Diagram (PIB Verification I Result update)

Table 2.6.2-3: Process Summary (PIB Verification I Result update)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ PIB declaration number ▫ Declared Office Code (Service office) ▫ Declared Date	CRT (Client)	• Update Window ▫ Name ▫ Address ▫ Part of PIB ▫ NPWP ▫ PIB Verification I Result	CRT (Client)	• PIB Verification I Result • DJBC Office • PIB Header • Basic Information • PIB Process • Code	(A) Processing Unit Processed on every PIB. (B) Processing Procedure (1) Retrieval of Verification Result I information When PIB declaration number, Declared Office Code and Declared Date are inputted, the Verification Result I information (before update), the PIB Header information and Basic Information will be retrieved. (2) Update of Verification Result I information When the correct verification result data is inputted into PIB Verification I Result update window, it will be checked and updated in PIB Verification I Result and PIB Verification Result Statistical. Instruction Note is printed out when necessary.	• Directorate must be Verification & Audit (inc. Regional Office).	—
2	• Update Window ▫ PIB Verification I Result (Correct information)	CRT (Client)	—	—	• PIB Verification I Result • PIB Verification II Result • PIB Verification Result Statistical			

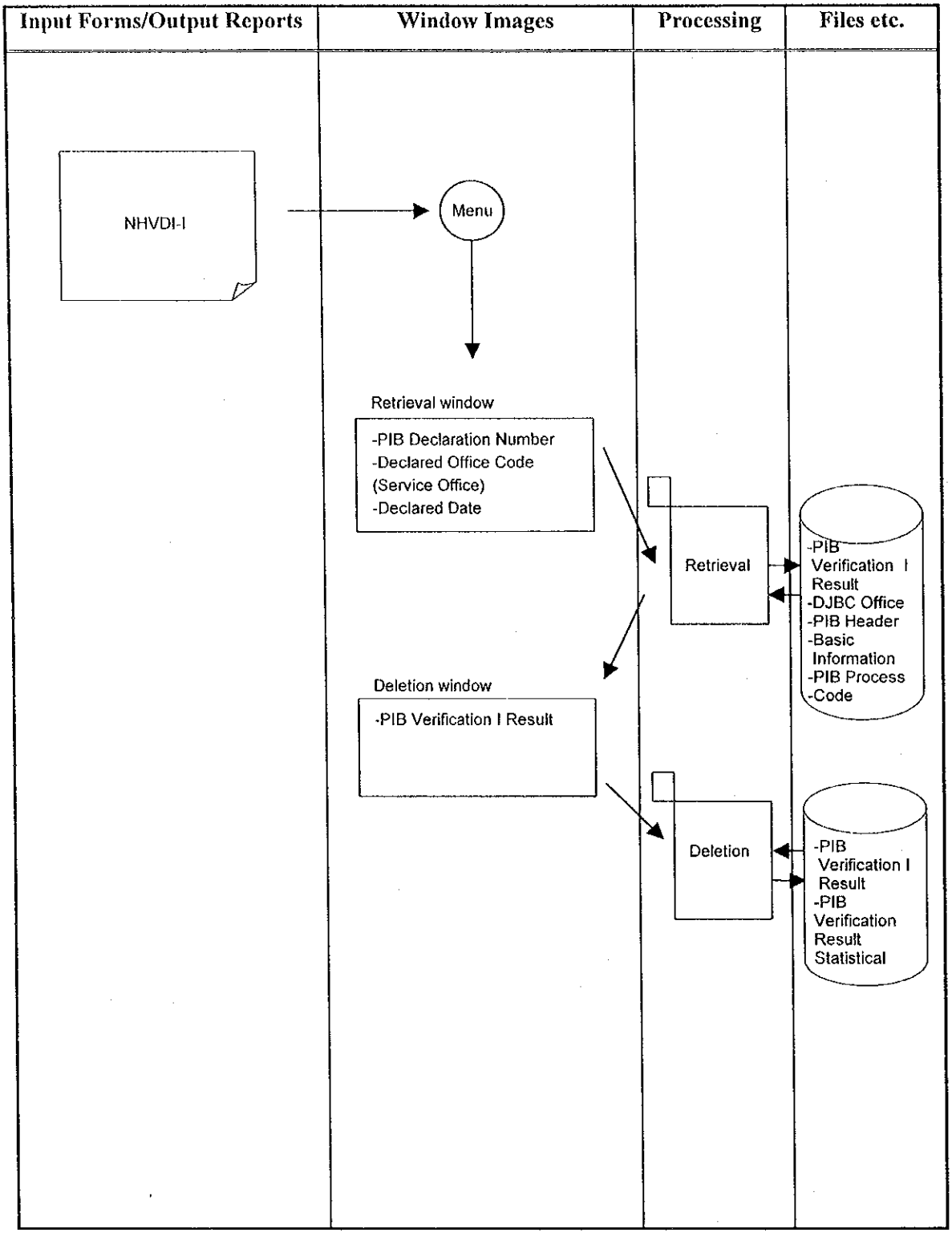

Figure 2.6.2-4: Process Diagram (PIB Verification I Result deletion)

Table 2.6.2-4: Process Summary (PIB Verification I Result deletion)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ PIB declaration number ▫ Declared Office Code (Service Office) ▫ Declared Date	CRT (Client)	• Deletion Window ▫ Verification result ▫ Name ▫ Address ▫ Part of PIB ▫ NPWP ▫ PIB Verification I Result	CRT (Client)	• PIB Verification I Result • DJBC Office • PIB Header • Basic Information • PIB Process • Code	(A) Processing Unit Processed on every PIB. (B) Processing Procedure (1) Retrieval of PIB Verification I Result information When PIB declaration number, Declared Office Code and Declared Date are inputted, the PIB Verification I Result information, the PIB Header information and Basic Information will be retrieved. (2) Deletion of PIB Verification I Result information When the confirmation to delete the result is done, the PIB Verification I Result information will be deleted and counted down from PIB Verification Result Statistical.	• Directorate must be Verification & Audit (inc. Regional Office). • PIB Verification I Result can not be deleted if linking information (NPWP, Regional Office Code, Verification II Date) is filled in. In this case, the related PIB Verification II Result must be deleted first, before PIB Verification I Result is deleted.	—
2	• Deletion Window ▫ Confirmation to delete	CRT (Client)	—	—	• PIB Verification I Result • PIB Verification Result Statistical			

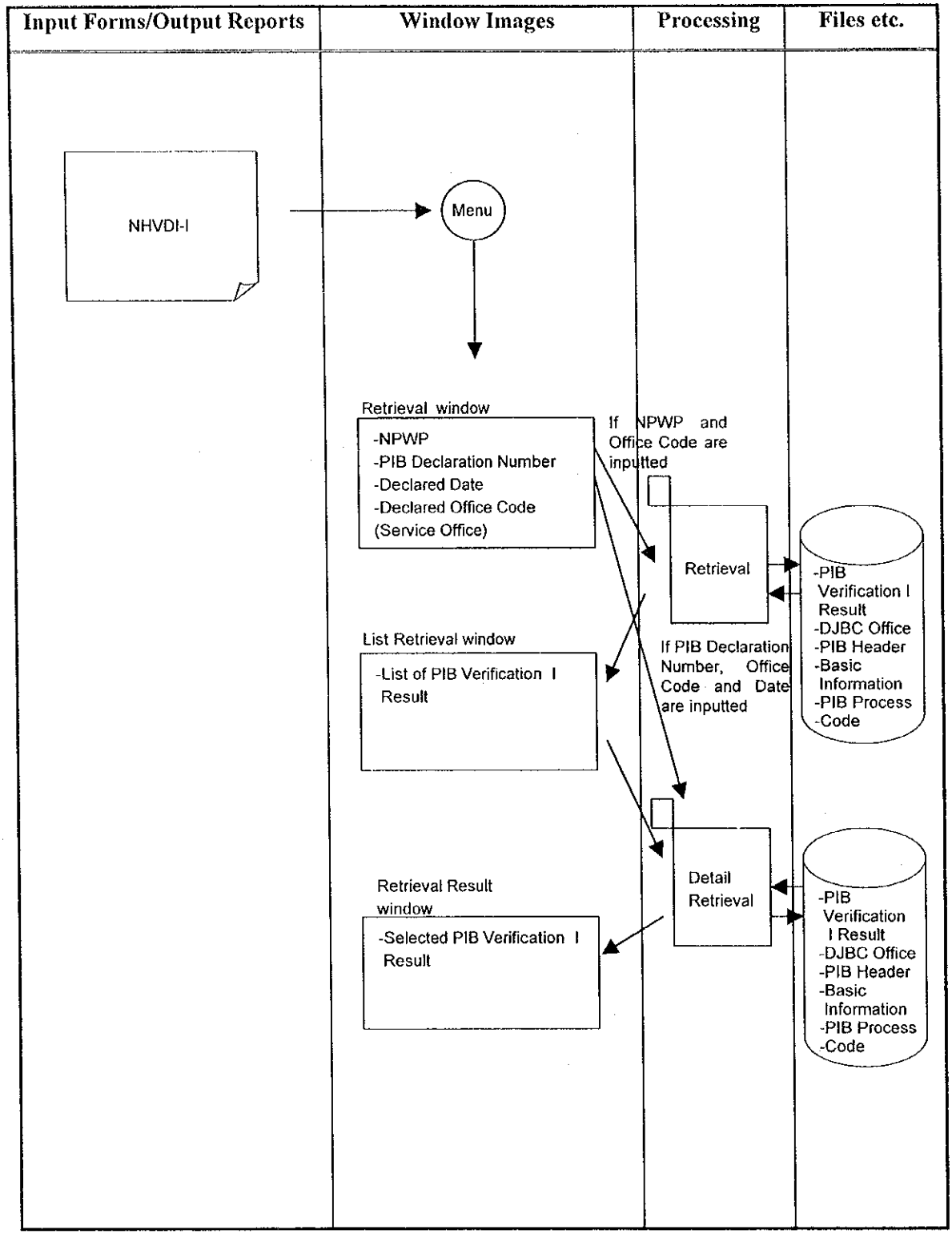

Figure 2.6.2-5: Process Diagram (PIB Verification I Result retrieval)

Table 2.6.2-5: Process Summary (PIB Verification I Result retrieval)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ PIB declaration number ▫ NPWP ▫ Declared Office Code (Service Office) ▫ Declared Date	CRT (Client)	• List Retrieval Window ▫ Name ▫ Address ▫ List of PIB Verification I Result	CRT (Client)	• PIB Verification I Result • DJBC Office • PIB Header • Basic Information • PIB Process • Code	(A) Processing Unit Processed when required. (B) Processing Procedure (1) Retrieval of Basic Information When NPWP number is inputted, the list of PIB Verification I Result information for that importer will be retrieved. (2) Retrieval of PIB Verification I Result information When the required PIB Verification I Result information is selected from the list in List Retrieval Window, the information will be retrieved.	• Directorate must be Verification & Audit (inc. Regional Office). • When PIB declaration number, Declared Service Office Code and Declared Date are inputted in Retrieval Window, the output is the Retrieval Result Window.	—
2	• List Retrieval Window ▫ Selection of required PIB Verification I Result	CRT (Client)	• Retrieval Result Window ▫ Selected PIB Verification I Result	CRT (Client)	• PIB Verification I Result • DJBC Office • PIB Header • Basic Information • PIB Process • Code			

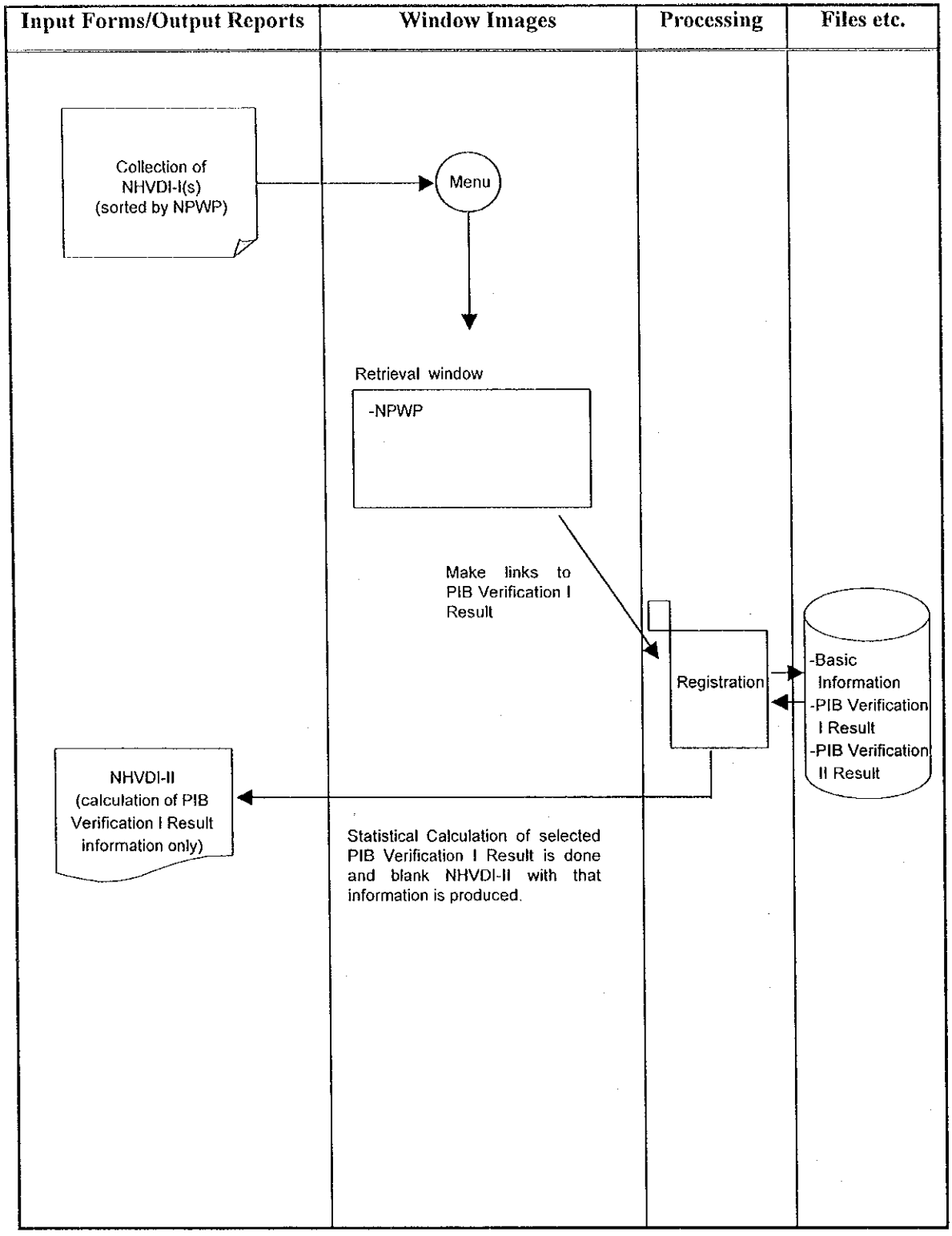

Figure 2.6.2-6 : Process Diagram(PIB Verification II Result registration)

Table 2.6.2-6: Process Summary (PIB Verification II Result registration)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP	CRT (Client)	• NHVDI-II ▫ Name ▫ Address ▫ NPWP ▫ Date ▫ Regional Office Code ▫ Statistical Calculation of PIB Verification I Result.	Printer (Client)	• Basic Information • PIB Verification I Result • PIB Verification II Result	(A) Processing Unit Processed on every certain amount of PIB Verification I Result. (B) Processing Procedure Registration of PIB Verification II Result. When NPWP is inputted, these steps will be done: (1) Look for PIB Verification I Results that are not updated by PIB Verification II Result registration process in PIB Verification I Result. (2) Extract necessary data from PIB Verification I Result and update PIB Verification I Result to make a link to PIB Verification II Result. (3) Register calculated statistical information and then print out NHVDI-II filled with calculation of PIB Verification I Result information only.	• Directorate must be Verification & Audit (only Regional Office can do this process).	• Verifier I will operate this process after certain amounts of PIB Verificat-ion I Result Registrat-ion. • The print out of NHVDI-II will be placed on top of the files of NHVDI-I and passed onto Verifier II.

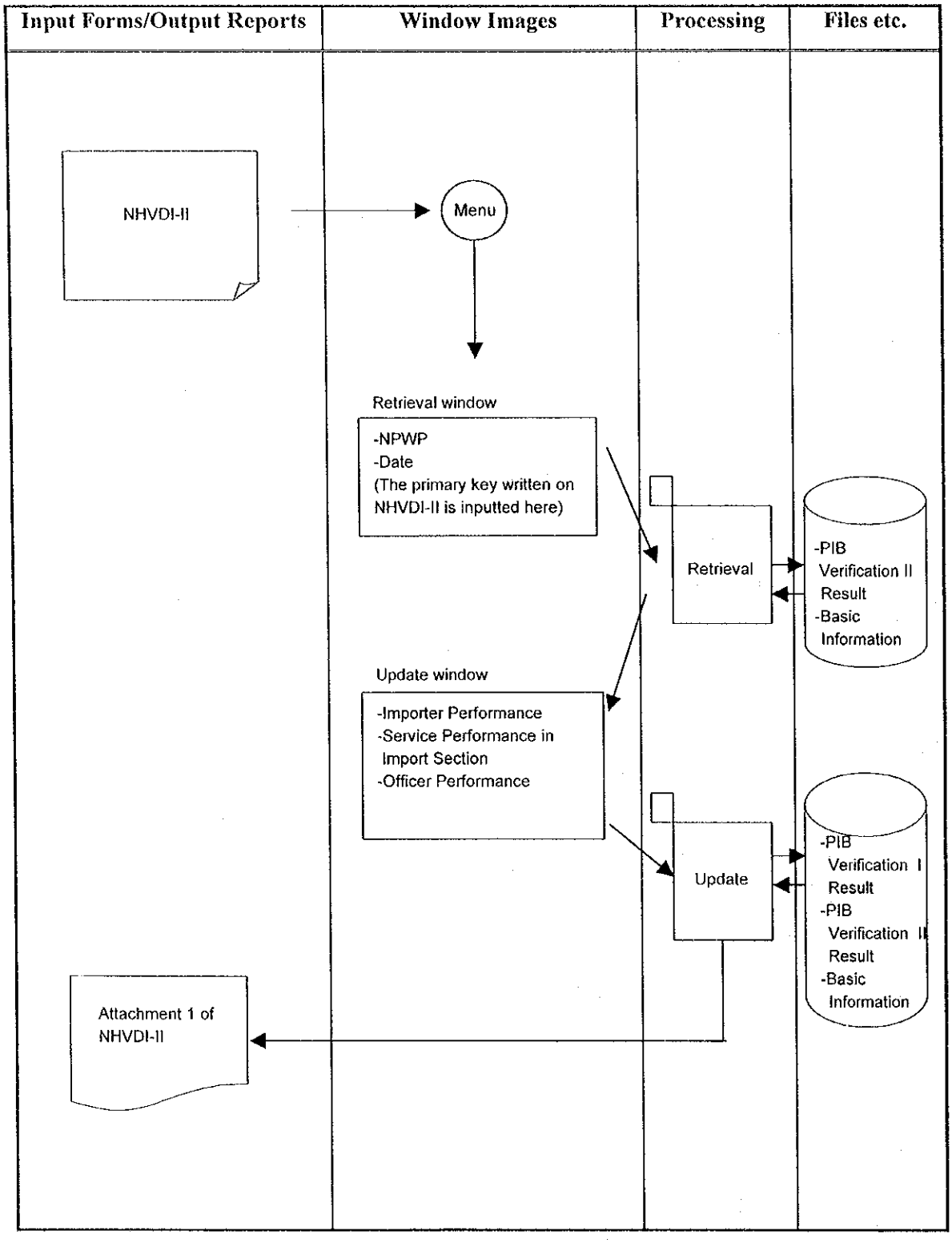

Figure 2.6.2-7 : Process Diagram (PIB Verification II Result update)

Table 2.6.2-7 : Process Summary (PIB Verification II Result update)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP ▫ Date	CRT (Client)	• Update Window ▫ Importer Performance ▫ Service Performance in Import Section ▫ Officer Performance	CRT (Client)	• PIB Verification II Result • Basic Information	(A) Processing Unit Processed on every PIB Verification II Result. (B) Processing Procedure (1) Retrieval of PIB Verification II Result When NPWP and Date are inputted, the company basic information and the PIB Verification II Result will be retrieved to Update Window. (2) Update of Verification II Result When the correct verification result data is inputted into PIB Verification II Result update window, it will be checked and updated in PIB Verification II Result. (3) User then can print or preview the Attachment I of NHVDI-II if required.	• Directorate must be Verification & Audit (only Regional Office can do this process).	This process is used not only for correcting information in PIB Verification II Result, but also used for registration. It means the unfilled information in PIB Verification II Result will be inputted in Update Window after verifier fill the NHVDI-II completely.
2	• Update Window ▫ Importer Performance ▫ Service Performance in Import Section ▫ Officer Performance	CRT (Client)	• Attachment I of NHVDI-II ▫ List of PIB Number ▫ Goods Description ▫ Quantity of goods ▫ Weight of goods ▫ Packing ▫ Invoice Validation ▫ Additional Payment / Refund	Printer (Client)	• PIB Verification I Result • PIB Verification II Result • Basic Information			

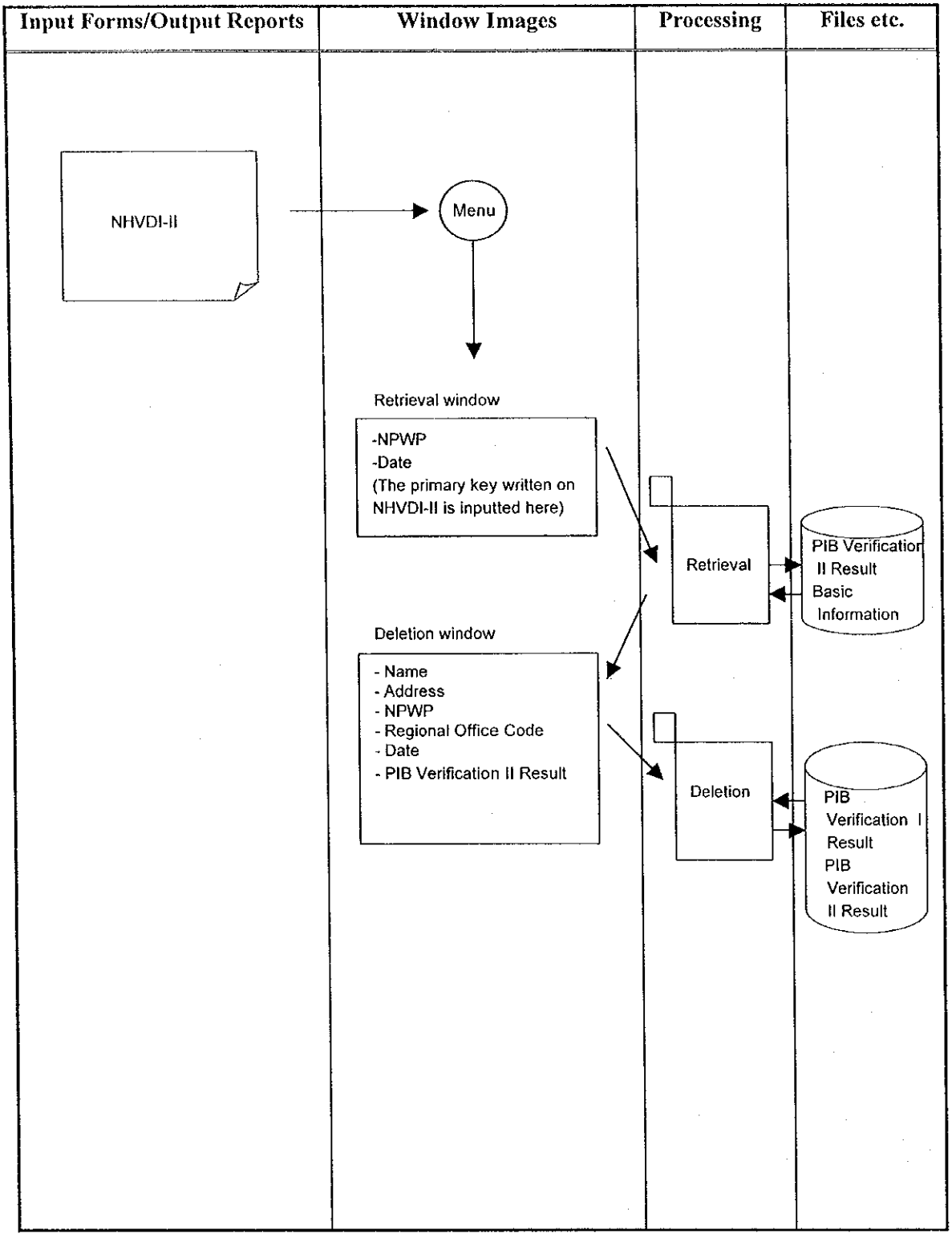

Figure 2.6.2-8 : Process Diagram (PIB Verification Result II deletion)

Table 2.6.2-8 : Process Summary (PIB Verification II Result deletion)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP ▫ Date	CRT (Client)	• Deletion Window ▫ Name ▫ Address ▫ NPWP ▫ Date ▫ PIB Verification II Result	CRT (Client)	• PIB Verification II Result • Basic Information	(A) Processing Unit Processed on every PIB Verification Result II. (B) Processing Procedure (1) Retrieval of PIB Verification Result II Information When NPWP and Date of Verification are inputted, Basic Information and PIB Verification II Result information will be retrieved. (2) Deletion of PIB Verification II Result Information When the confirmation to delete the result is done, the PIB Verification II Result will be deleted in PIB Verification II Result. Update the related information in PIB Verification I Result by removing the links, so there is no linking to PIB Verification II Result.	• Directorate must be Verification & Audit (only Regional Office can do this process).	—
2	• Deletion Window ▫ Confirmation to delete	CRT (Client)	—	—	• PIB Verification I Result • PIB Verification II Result			

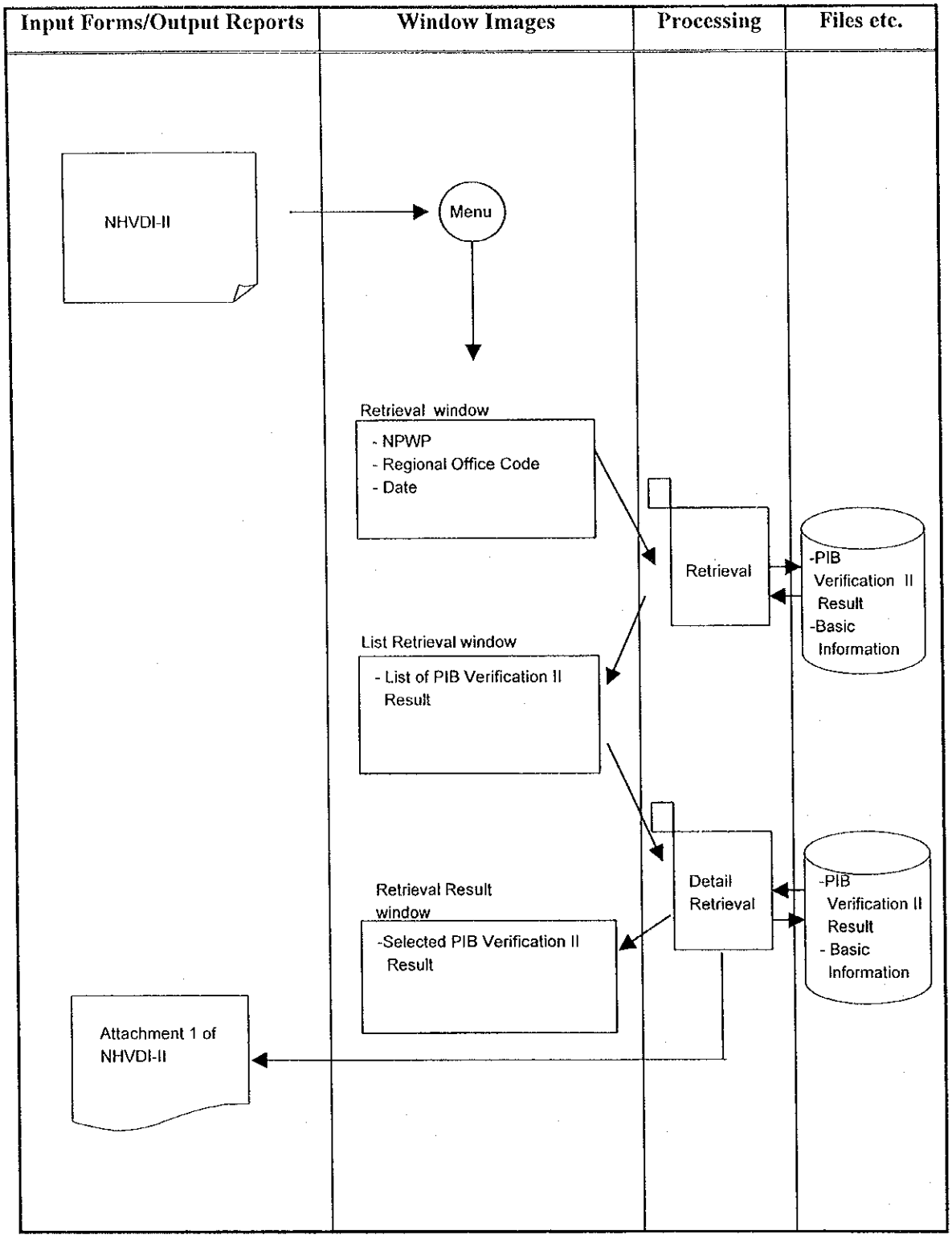

Figure 2.6.2-9: Process Diagram (PIB Verification II Result retrieval)

Table 2.6.2-9: Process Summary (PIB Verification II Result retrieval)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP ▫ Regional Office Code ▫ Date	CRT (Client)	• List Retrieval Window ▫ List of PIB Verification II Result	CRT (Client)	• Basic Information • PIB Verification II Result	(A) Processing Unit Processed when required. (B) Processing Procedure (1) Retrieval of List of PIB Verification II Result When NPWP, Regional Office Code and Date is inputted, the list of PIB Verification II Result for that importer will be retrieved from PIB Verification II Result. (2) Retrieval of details PIB Verification II Result. When the required PIB Verification II Result is selected from the list in List Retrieval Window, the information will be retrieved. (3) User then can print or preview the Attachment I of NHVDI-II if required.	• Directorate must be Verification & Audit (inc. Regional Office and Head office).	—
2	• List Retrieval Window ▫ Selection of required PIB Verification II Result	CRT (Client)	• Retrieval Result Window ▫ Selected PIB Verification II Result • Attachment I of NHVDI-II ▫ List of PIB Number ▫ Goods Description ▫ Quantity of goods ▫ Weight of goods ▫ Packing ▫ Invoice Validation ▫ Additional Payment / Refund	CRT (Client)	• PIB Verification I Result • PIB Verification II Result • Basic Information			

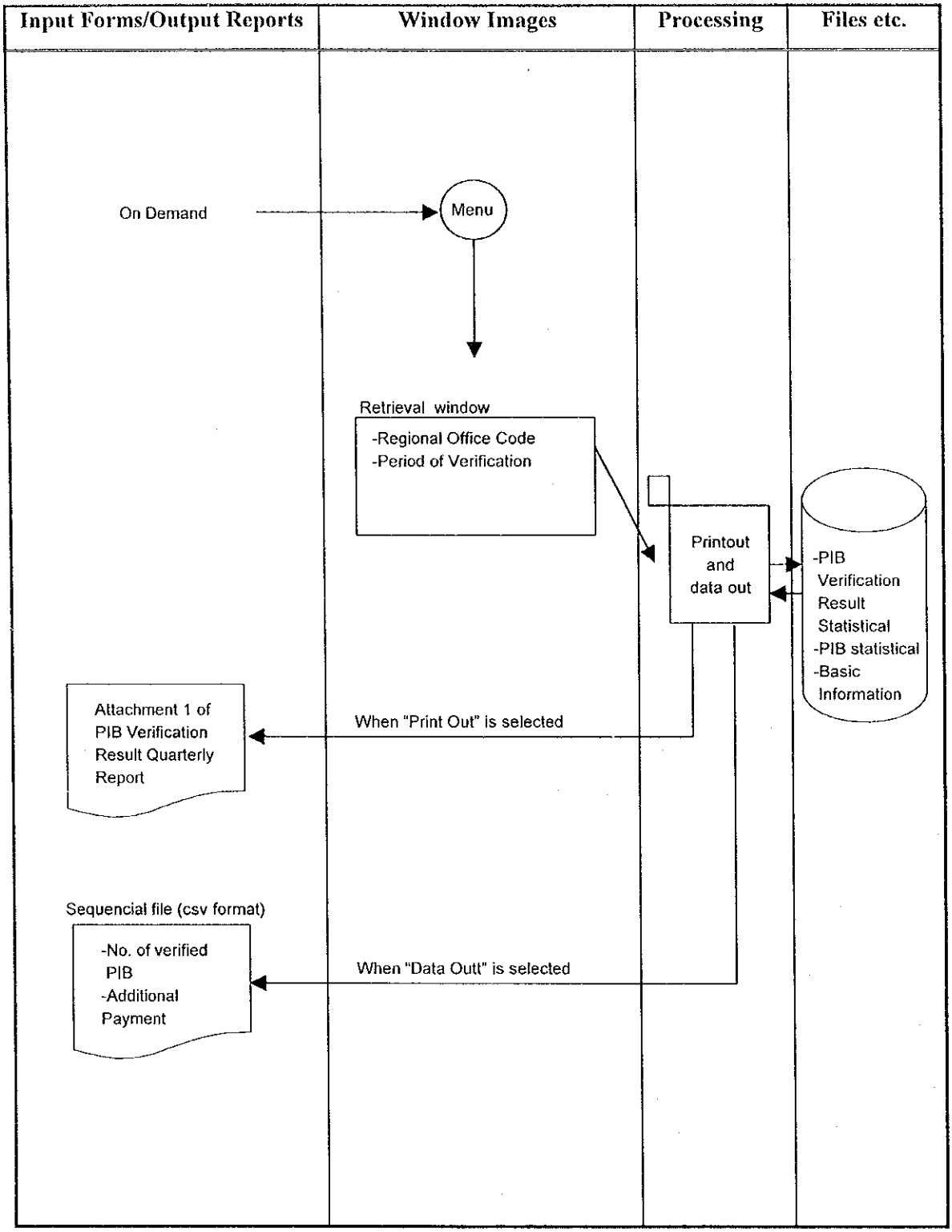

Figure 2.6.2-10: Process Diagram (PIB Verification Result Quarterly Report A1 retrieval)

Table 2.6.2-10: Process Summary (PIB Verification Result Quarterly Report A1 retrieval)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ Regional Office Code ▫ Period of Verification	CRT (Client)	• Attachment 1 of PIB Verification Result Quarterly Report ▫ Number of noncompliances ▫ Additional Payment	Printer (Client) Storage Device (Client)	• PIB Verification Result Statistical • PIB Statistical • Basic Information	(A) Processing Unit Processed by each Regional Office (B) Processing Procedure (1) Retrieval of PIB Verification Result Quarterly Report information. When Office Code and Period of Verification is inputted, the application will print attachment 1 of PIB Verification Result Quarterly Report to local printer, or transfer retrieved data to the storage device of client computer, depending on the check box on the retrieval window. This report is the statistical result of many items taken from PIB Verification I Result and PIB Statistical.	• Directorate must be Verification & Audit (inc. Regional Office).	—

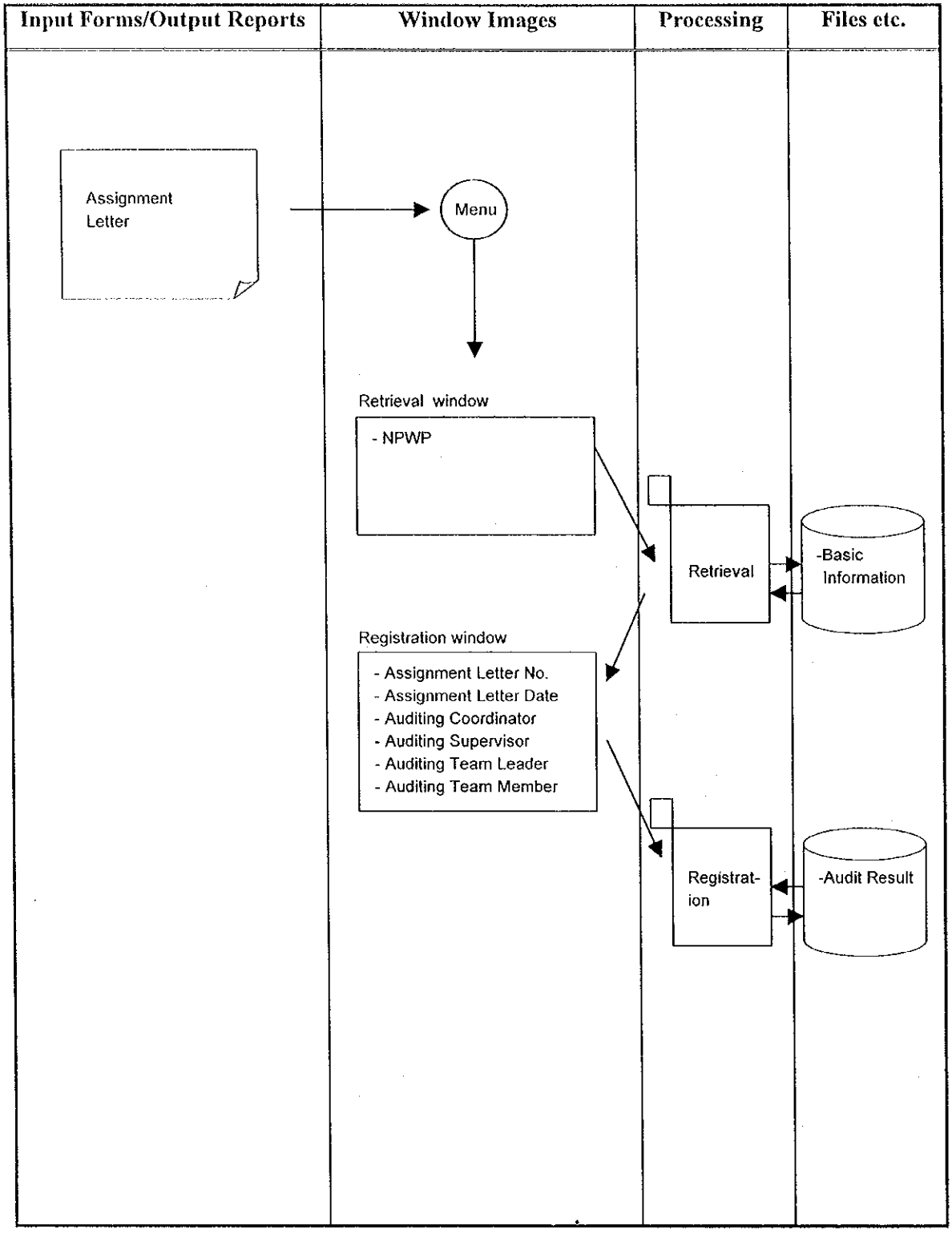

Figure 2.6.2-11: Process Diagram (Audit Result registration)

Table 2.6.2-11: Process Summary (Audit Result registration)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP	CRT (Client)	• Registration Window ▫ Name ▫ Address ▫ SIUP No. ▫ Part of Basic Information	CRT (Client)	• Basic Information	(A) Processing Unit Processed on every first step of Audit. (B) Processing Procedure (1) Retrieval of NPWP Information When NPWP number is inputted, the Basic Information will be retrieved. (2) Registration of Audit Result Information When Assignment Letter No. is inputted into Audit Result registration window, check and register the information in Audit Result.	• Directorate must be Verification & Audit (inc. Regional Office). • Assignment Letter No. must not be existed in Audit Result.	The process is carried out after the decision to audit a company before audit conducting.
2	• Registration Window ▫ Assignment Letter No. ▫ Assignment Letter Date ▫ Auditing Coordinator ▫ Auditing Supervisor ▫ Auditing Team Leader ▫ Auditing Team Member	CRT (Client)	—	—	• Audit Result			

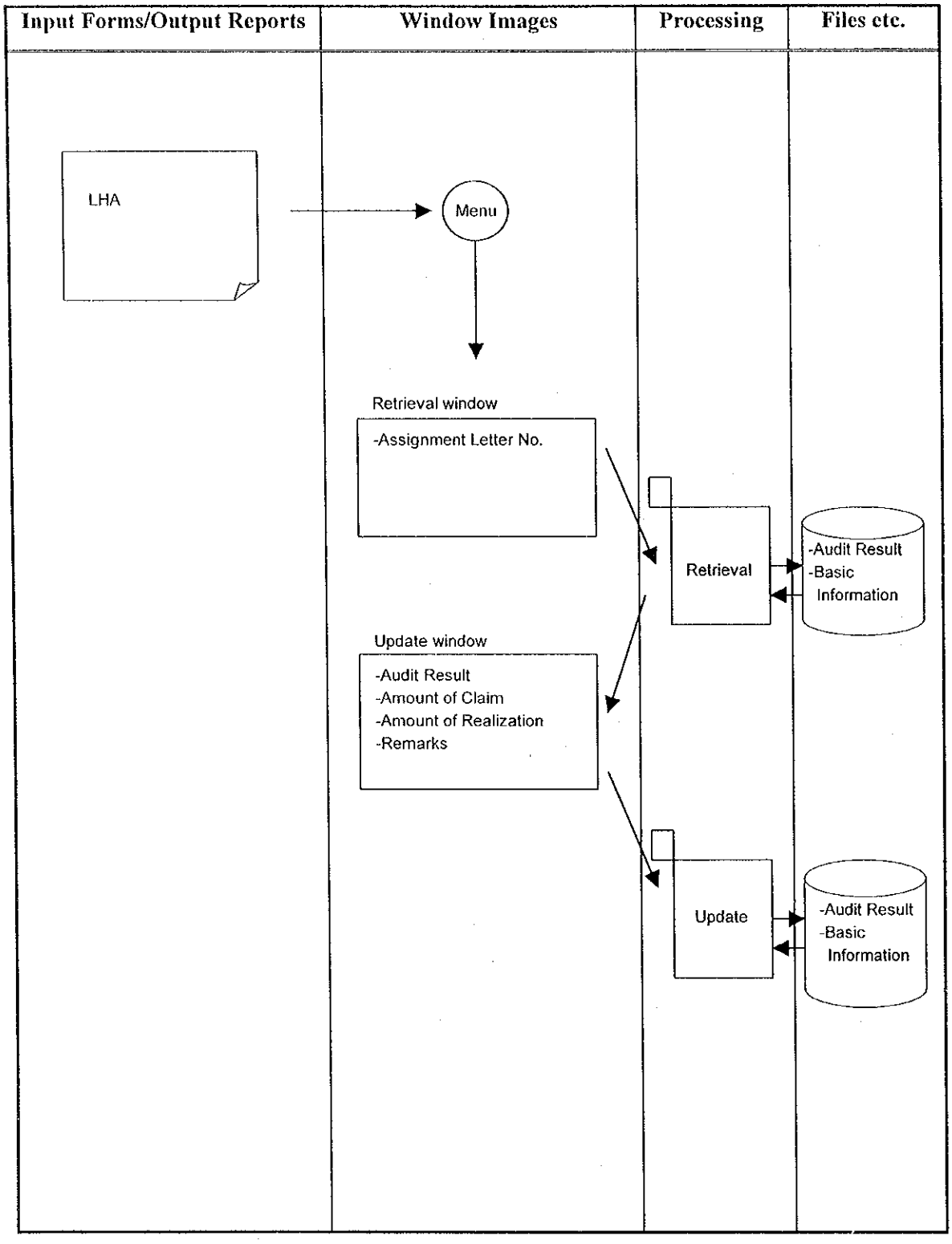

Figure 2.6.2-12: Process Diagram (Audit Result update)

Table 2.6.2-12: Process Summary (Audit Result update)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ Assignment Letter No.	CRT (Client)	• Update Window ▫ NPWP ▫ Name ▫ Address ▫ Audit Result	CRT (Client)	• Audit Result • Basic Information	(A) Processing Unit Processed on every step of Audit Result. (B) Processing Procedure (1) Retrieval of Audit Result Information When Assignment Letter No. is inputted, the Audit Result Information and NPWP will be retrieved and based on the NPWP, Basic Information will be retrieved. (2) Update of Audit Result Information When the Audit Result data is inputted into Audit Result update window it will be checked and updated in Audit Result.	• Directorate must be Verification & Audit (inc. Regional Office). • An Assignment Letter No. must exist.	When company profile needs updating, request P2 Directo-rate for update. The Process is used not only for correct-ing Audit Result, but also used for Registra-tion.
2	• Update Window ▫ Audit Result	CRT (Client)	—	—	• Audit Result • Basic Information			

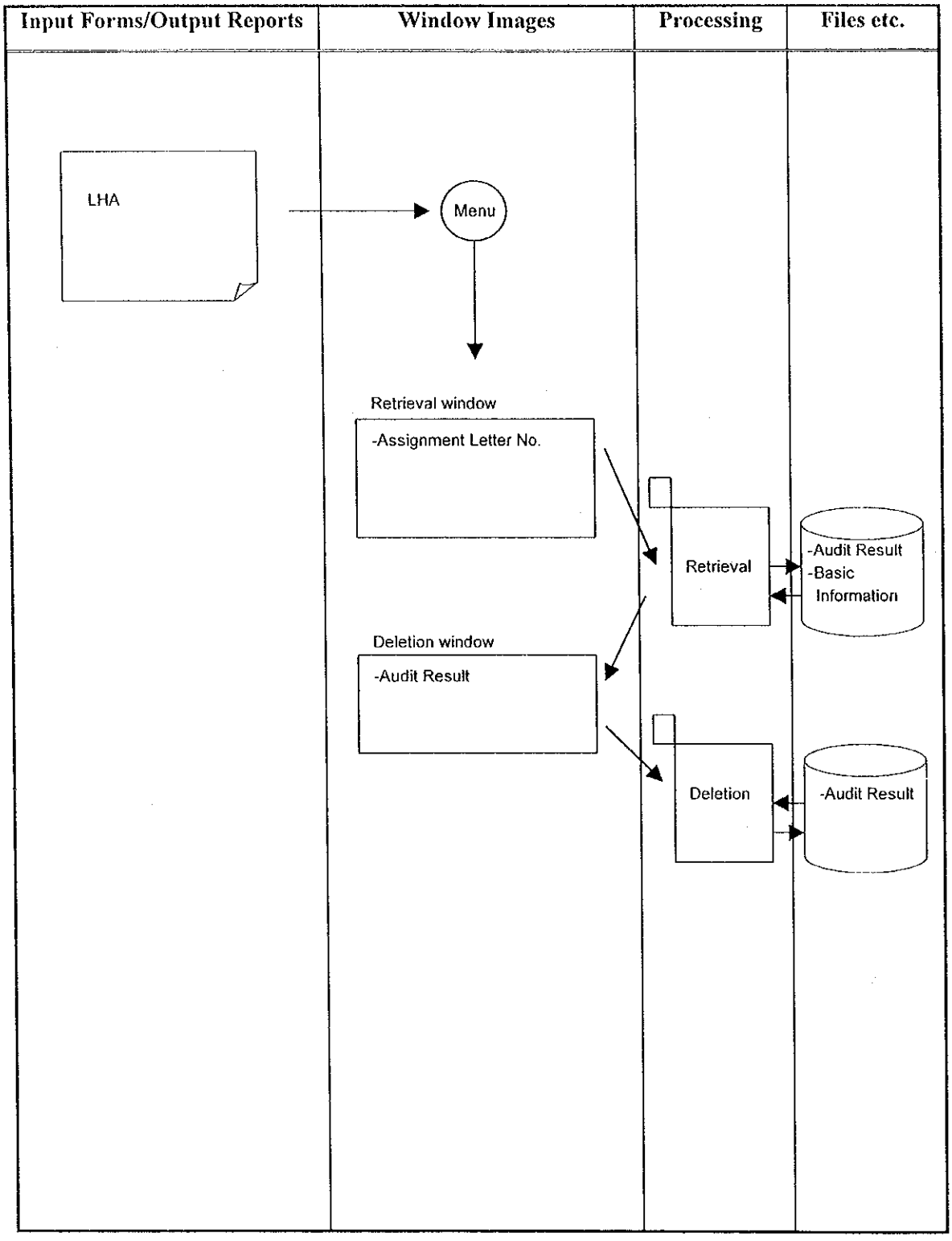

Figure 2.6.2-13: Process Diagram (Audit Result deletion)

Table 2.6.2-13: Process Summary (Audit Result deletion)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ Assignment Letter No.	CRT (Client)	• Deletion Window ▫ Name ▫ Address ▫ Audit Result	CRT (Client)	• Audit Result • Basic Information	(A) Processing Unit Processed on every Assignment Letter No. (B) Processing Procedure (1) Retrieval of Audit Result Information When Assignment Letter No. is inputted, the Audit Result Information and NPWP will be retrieved, and based on the NPWP, Basic Information will be retrieved. (2) Deletion of Audit Result Information When the confirmation to delete the result is done, the Audit Result Information will be deleted.	• Directorate must be Verification & Audit (inc. Regional Office).	—
2	• Deletion Window ▫ Confirmation to delete	CRT (Client)	—	—	• Audit Result			

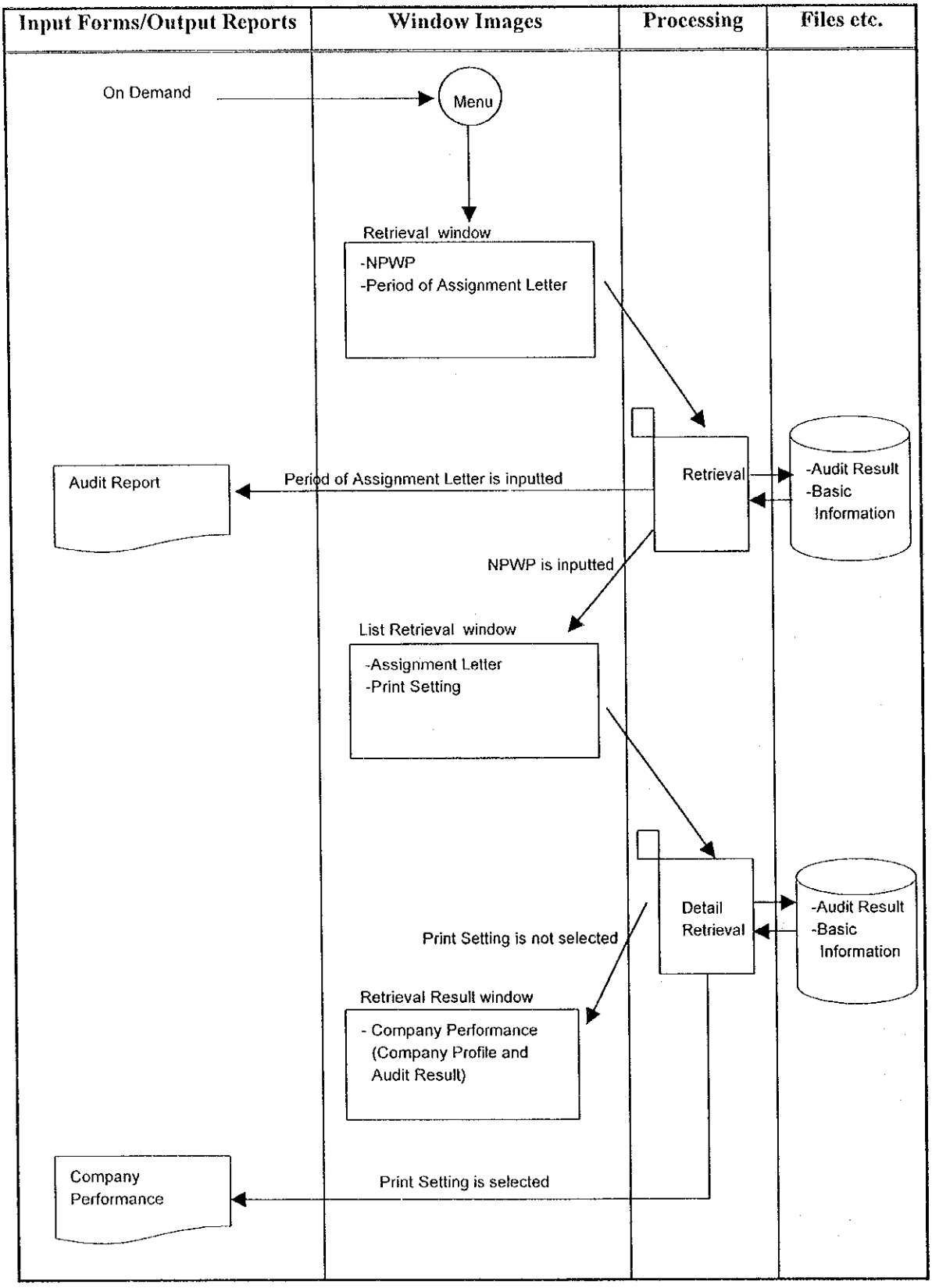

Figure 2.6.2-14: Process Diagram (Audit Result Retrieval)

Table 2.6.2-14: Process Summary (Audit Result retrieval)

No.	Input		Output		Files	Process Procedure	Process Condition	Notes
	Input Data	Input from:	Output Data	Output to:				
1	• Retrieval Window ▫ NPWP ▫ Period of Assignment Letter	CRT (Client)	• List Retrieval Window	CRT (Client)	• Audit Result • Basic Information	(A) Processing Unit Processed on every company or period of Assignment Letter. (B) Processing Procedure (1) Retrieval of List Retrieval Window When NPWP number is inputted, retrieve Basic Information and Audit Result then display the List of Retrieval Window. When period of Assignment Letter is inputted, Audit Report during the inputted period is printed out in the form of list. (2) Select the Assignment Letter No. When Print Setting is not selected, then display Retrieval Result Window. When Print Setting is selected, then print out Company Performance.	• User can only input one item, NPWP or Period of Assignment Letter. • Directorates other than Verification & Audit are not able to select "Period of Assignment Letter" when input.	—
			• Audit Report ▫ Company Name ▫ Assignment Letter	Printer (Client)				
2	• List Retrieval Window ▫ Assignment Letter ▫ Print Setting	CRT (Client)	• Retrieval Result Window ▫ Basic Information ▫ Assignment Letter ▫ Finding Result	CRT (Client)	• Audit Result • Basic Information			
			• Company Performance (Company Profile and Audit Result) ▫ Basic Information ▫ Assignment Letter ▫ Finding Result	Printer (Client)				

Table 2.6.2-15: List of Windows (1/2)

No.	Window Code	Window Name	Input/ Output			Window Type	Note
			Input & Output	Input	Output		
1	WV011010	PIB Verification I Result Registration (Retrieval Window)		✓		Card Pattern	—
2	WV011020	PIB Verification I Result Registration (Registration Window)	✓			Card Pattern	—
3	WV012010	PIB Verification I Result Update (Retrieval Window)		✓		Card Pattern	—
4	WV012020	PIB Verification I Result Update (Update Window)	✓			Card Pattern	—
5	WV013010	PIB Verification I Result Deletion (Retrieval Window)		✓		Card Pattern	—
6	WV013020	PIB Verification I Result Deletion (Deletion Window)	✓			Card Pattern	—
7	WV014010	PIB Verification I Result Retrieval (Retrieval Window)		✓		Card Pattern	—
8	WV014020	PIB Verification I Result Retrieval (List Retrieval Window)	✓			List Pattern	—
9	WV014030	PIB Verification I Result Retrieval (Retrieval Result Window)			✓	Card Pattern	—
10	WV021001	PIB Verification II Result Registration (Retrieval Window)		✓		Card Pattern	—
11	WV022001	PIB Verification II Result Update (Retrieval Window)		✓		Card Pattern	—
12	WV022002	PIB Verification II Result Update (Update Window)	✓			Card Pattern	—
13	WV023001	PIB Verification II Result Deletion (Retrieval Window)		✓		Card Pattern	—
14	WV023002	PIB Verification II Result Deletion (Deletion Window)	✓			Card Pattern	—
15	WV024001	PIB Verification II Result Retrieval (Retrieval Window)		✓		Card Pattern	—
16	WV024002	PIB Verification II Result Retrieval (List Retrieval Window)	✓			List Pattern	—

Table 2.6.2-15: List of Windows (2/2)

No.	Window Code	Window Name	Input/ Output			Window Type	Note
			Input & Output	Input	Output		
17	WV024003	PIB Verification II Result Retrieval (Retrieval Result Window)			✓	Card Pattern	—
18	WV034010	PIB Verification Result Quarterly Report A1 Retrieval (Retrieval Window)		✓		Card Pattern	—
19	WV041010	Audit Result Registration (Retrieval Window)		✓		Card Pattern	—
20	WV041020	Audit Result Registration (Registration Window)	✓			Card Pattern	—
21	WV042010	Audit Result Update (Retrieval Window)		✓		Card Pattern	—
22	WV042020	Audit Result Update (Update Window)	✓			Card Pattern	—
23	WV043010	Audit Result Deletion (Retrieval Window)		✓		Card Pattern	—
24	WV043020	Audit Result Deletion (Deletion Window)	✓			Card Pattern	—
25	WV044010	Audit Result Retrieval (Retrieval Window)		✓		Card Pattern	—
26	WV044020	Audit Result Retrieval (List Retrieval Window)	✓			List Pattern	—
27	WV044030	Audit Result Retrieval (Retrieval Result Window)			✓	Card Pattern	—

Table 2.6.2-16: List of Reports

No.	Report Code	Report No.	Report Name	Output Place	Output Cycle	Report Type	Paper Size	Notes
1	RV011010	—	Instruction Note *Nota Dinas Tindak Lanjut*	Regio-nal Office	On demand	Card Pattern	A4	—
2	RV021010	—	NHVDI-II (calculation of PIB Verification I Result information only) *NHVDI-II (Perhitungan Hasil Verifikasi PIB I)*	Regio-nal Office	On demand	Card Pattern	A4	—
3	RV022010	—	Attachment 1 of NHVDI-II *Lampiran 1 NHVDI-II*	Regio-nal Office	Monthly	List Pattern	A3	—
4	RV034010	—	Attachment 1 of PIB Verification Result Quarterly Report *Lampiran 1 Laporan Triwulan Hasil Verifikasi*	Regio-nal Office	Quarter-ly	List Patern	A3	—
5	RV044010	—	Company Performance *Profil Perusahaan*	Head Office / Regio-nal Office	On demand	Slip Pattern	A3	—
6	RV044020	—	Audit Report *Laporan Audit*	Head Office	On demand	List Pattern	A3	—

CHAPTER 3 System Architecture Design

3.1 Outline of System Architecture

3.1.1 Circumstances

The purpose of CIS is to provide high quality risk management in order to realize prompt and proper customs procedure by controlling all customs information and intelligence at one place and analyzing them. Considering the purpose of CIS, CIS has to be connected to the Wide Area Network (hereinafter referred to as WAN) in order to exchange information among the offices and access to the CIS information from each office. Networking capability should be a first priority among the CIS hardware requirements. Reliability, expandability and performance should be considered regarding the CIS hardware. Introduction of appropriate security system should also be considered to protect the confidential customs information.

DJBC would like to use the existing server machines as the CIS servers in order to reduce the CIS development cost. As the results of the comparison of the CIS server requirement (refer to 3.8.2), the existing server in Head office fulfills the specification of the CIS Main Server at the Head Office. However, the existing server is being used as the server for developing and maintaining the application programs of DJBC. Therefore, it is very difficult to use it as the Main Server and the JICA Study Team recommends installing a new machine for the Main Server. The servers of Regional Office IV, V, and VII do not satisfy the requirements and have to be replaced. Nine other Regional Offices are expected to use their existing servers for the CIS Regional Servers by first adding memory and disks.

The JICA Study Team designed the CIS Main Server as a part of the scope of work; however, Regional Servers have only been roughly estimated for their specification in order to roughly estimate the CIS development cost at this time. The detail design of Regional Server should be needed in later stage of the CIS development, and the existing server machines have to be evaluated in more detail at that time by the vendor.

Chapter 3 in Volume II of this report mainly explains the system architecture requirements of DJBC and the basic design and detail design of system configuration at the first stage, such as the CIS Main Server, the CIS terminals, LAN, and WAN. They are supposed to be the procurable equipment or services as of November in 1998. On the other hand, some parts of chapter 3 mention the system configuration in the second and third stage as the results of the basic investigation in order to clear the final image of the CIS configuration and to estimate the total CIS development cost.

The JICA Study Team has tried to take account the concept of open system into the CIS system architecture in this report. However, some parts of these designs might be modified or updated after choosing the certain vendors, since the system architecture depends on the hardware or the software of each vendor. The JICA Study Team would like to recommend that DJBC check the results of this research and request vendors the latest products including the latest technology, when DJBC chooses the certain vendors.

3.1.1.1 Summary of requirements

Table 3.1.1.1-1 shows the summary of user requirements for CIS based on interviews and questionnaire results (refer to later section). As the result of hearing, required number of main equipment, such as Main Server, Regional Server, and personal computer in each stage are shown in Table 3.1.1.1-2.

Terminal locations of each office at the first stage are shown in Table 3.1.1.1-2 to 3.1.1.1-7. This number of PC and locations are based on the results of investigation on October, 1998. If the organization of DJBC or the location of each section is changed, those number or locations should be re-considered.

In the second and third stages, five PCs and one printer are supposed to be needed in each Regional office, and three PCs and one printer are supposed to be needed in each Service Office. In addition, the locations of CIS terminals installed at the second and third stages should be investigated before starting each stage.

Table 3.1.1.1-1: Summary of requirements

Items	Requirements
Network	• Each computer for CIS in one location connects to the Local Area Network in that location. • LAN to LAN interconnection of CIS is built as a closed Wide Area Network, connecting Head Office, 12 Regional Offices, and some of major Service Offices. • Networking infrastructure supports on-line process.
Hardware	• Dual computer system for the Main Server in Head Office(hereinafter referred to as Main Server), one for active computer, the other for stand-by computer. • CIS Regional Server is single computer system. • CIS terminal should be Personal Computer (hereinafter referred to as PC).
Security	• CIS users are grouped by Directorate, Regional Office, and Service Office. They have different permission level to access CIS. • Users in the same Directorate have the same set of privileges and restrictions to CIS. • Directorate of Central of Automated Data and Information Processing (hereinafter referred to as ADP) staffs are responsible for user administration.
Operation and Maintenance	• CIS Main Server runs 24 hours a day, 7 days a week. CIS is available to the end-users only during the working hours. • On-line maintenance for CIS is available. • For maintenance of CIS, sophisticated maintenance tool is required, such as job scheduler function, system monitor function, resources distribution.
Others	• Utilization of existing server machines in Regional Offices should be considered. • CIS connects to Customs Fast Release System (hereinafter referred to as CFRS) or Customs Services System (hereinafter referred to as CSS).*

Note: "CFRS" is current computer system of DJBC. CSS would be a re-designed computer system of CFRS in the future. Therefore, CFRS would mean CSS also, regarding System Architecture in the later part of this report. Nevertheless, CSS function might be different from CFRS function.

Table 3.1.1.1-2: Number of main equipment (1/2)

Equipment	Definition	First stage	Second stage	Third stage	Total
Main Server	High performance & High reliability server machine.	1 Head Office	—	—	1
Regional Server Type I	Type I is categorized as large size Regional Server for CIS.	—	1 Regional Office IV (Jakarta)	—	1
Regional Server Type II	Type II is categorized as middle size Regional Server for CIS.	—	2 Regional Office V (Bundung) Regional Office VII (Surabaya)	—	2
Regional Server Type III	Type III is categorized as small size Regional Server for CIS. It is expected to use existing servers.	—	2 Regional Office I Medan Regional Office VI Semarang	7 Regional Office II (Balai Karimun) Regional Office III (Palembang) Regional Office VIII (Denpasar) Regional Office IX (Pontianak) Regional Office X (Balikpapan) Regional Office XI (Ujung Pandang) Regional Office XII (Ambon)	9
EUC Server	Dedicated sever for EUC function.	1 Head Office	—	—	1

Table 3.1.1.1-2: Number of main equipment (2/2)

Equipment	Definition	First stage	Second stage	Third stage	Total
Terminal / Printer	Personal computer for CIS terminal and Printer	95 PCs/45 Printers Head office (55/23) • Regional Office Regional Office IV (Jakarta) (14/7) • Service Office Tanjung Priok I (8/5) Tanjung Priok II (10/5) Tanjung Priok III (8/5)	35 PCs/9 Printers • Regional Office Regional Office I (Medan) (5/1) Regional Office VI (Semarang) (5/1) Regional Office V (Bandung) (5/1) Regional Office VII (Surabaya) (5/1) • Service Office Belawan (3/1) Soekarno Hatta II (3/1) Bandung (3/1) Tanjung Emas (3/1) Tanjung Perak (3/1)	35 PCs/7 Printers • Regional Office Regional Office II (Balai Karimun) (5/1) Regional Office III (Palembang) (5/1) Regional Office VIII (Denpasar) (5/1) Regional Office IX (Pontianak) (5/1) Regional Office X (Balikpapan) (5/1) Regional Office XI (Ujung Pandang) (5/1) Regional Office XII (Ambon) (5/1)	165PCs /61 Printers

Table 3.1.1.1-3: Terminal Location in Head Office

No	Directorate	Subdirectorate/Division	Building	Floor	Number of PC for CIS	Remark
1	Revenue Planning	—	A	4th	3	2 printers
2	Customs Technique	—	A	Ground	4	3 printers
3	Customs Facilitation	—	A	3rd	3	2 printers
4	International Affairs	—	A	1st	1	1 printer
5	Excise	—	B	4th	3	2 printers
6	Prevention and Investigation	Intelligence	B	3rd	20	4 printers
		Enforcement	B	2nd	3	1 printer
		Prohibited and Restricted Goods Supervising	B	3rd	3	1 printer
		Investigation	B	3rd	3	1 printer
7	Verification and Audit	—	B	2nd	5	2 printers
8	Central of Automated Data and Information Processing	—	C	2nd	5	Including extra PC in case of breakdown. 3 printers.
9	International Affair	—	C	1st	2	1 printer
Total PCs and Printers					55	23 printers

Table 3.1.1.1-4: Terminal Location in Regional Office IV

No	Division	Section	Floor	Number of PC for CIS	Remark
1	Customs & Excise	Import Section Export & Excise	2nd	1	1 printer
2	Prevention & Investigation	Intelligent Investigation Measure Operation Facilities	3rd	4	2 printers
3	Verification	Import Verification Export & Excise Verification	2nd	6	2 printers
4	Audit	Import Audit Export & Excise Audit	1st	2	1 printer
5	Head of Regional Office	—	4th	1	1 printer
		Total PCs and Printers		14	7 printers

Table 3.1.1.1-5: Terminal Location in Service Office Tanjung Priok I (Gedung Induk)

No	Section	Subsection	Floor	Number of PC for CIS	Remark
1	Manifest & Information	Completion & Acceptance Manifest	3rd	4	1 printer
		Means of Transport Inspection			
		Information			
2	Treasury	Revenue Manage & Deferred Guarantee	4th	1	1 printer
		Collection & Reimbursement			
3	Customs	Warehouse	3rd	1	1 printer
		Hangar			
4	Head of KPBC 1	—	2nd	1	1 printer
5	Document Distribution & Computer Operational	Computer Operational	3rd	1	1 printer
		Preparation Data & Information			
		Distribution			
			Total PCs and Printers	8	5 printers

Table 3.1.1.1-6: Terminal Location in Service Office Tanjung Priok II (Unit Terminal Peti Kemas)

No	Section	Subsection	Floor	Number of PC for CIS	Remark
1	Manifest & Information	Completion & Acceptance Manifest	3rd	6	1 printer
		Means of Transport Inspection			
		Information			
2	Treasury	Revenue Manage & Deferred Guarantee	2nd	1	1 printer
		Collection & Reimbursement			
3	Customs	Warehouse	2nd	1	1 printer
		Hangar			
4	Document Distribution & Computer Operational	Computer Operational	1st	1	1 printer
		Preparation Data & Information			
		Distribution			
5	Head of KPBC 2	—	2nd	1	1 printer
			Total PCs and Printers	10	5 printers

Table 3.1.1.1-7: Terminal Location in Service Office Tanjung Priok III (Gedung Induk)

No	Section	Subsection	Floor	Number of PC for CIS	Remark
1	Manifest & Information	Completion & Acceptance Manifest Means of Transport Inspection Information	4th	4	• Hub available • 1 printer
2	Treasury	Revenue Manage & Deferred Guarantee Collection & Reimbursement	3rd	1	1 printer
3	Customs	Warehouse Hangar	3rd	1	1 printer
4	Head of KPBC 3	—	2nd	1	1 printer
5	Document Distribution & Computer Operational	Computer Operational Preparation Data & Information Distribution	5th	1	1 printer
			Total PCs and Printers	8	5 printers

3.1.2 Concept of system configuration

CIS will be a huge system that connects all Regional Offices and 8 major Service Offices all over Indonesia in order to enable these offices to exchange information at the final stage. CIS should be protected by reliable security system to store highly confidential customs information. CIS has to able to make the current Customs business process faster and more efficient.

Here is the concept of CIS configuration, considering above-mentioned condition:

- Network connection in each offices by high-speed and reliable line.
- The system operates 24 hours a day and 7 days a week in Head Office.
  CIS is available to the end-users only during the working hours.
- Open system (Unix, Oracle, Network, and so on).
- Highly reliable system.
- User friendly system operation (Graphic User Interface).
- Remote maintenance and monitoring.
- Closed and secure information system.
- Database constructed on standard products in the industry.
- Connected to CFRS (CSS) network.

Considering the reliability, scalability, security, and performance factors of CIS, the JICA Study Team proposes the following design directions:

- To realize the connection by high-speed and reliable line among offices, digital line provided by ISDN or Leased Line facility is recommended in the first stage.
- To realize the Open System in CIS, standard Unix operating system, standard relational database Oracle and standard network protocol TCP/IP are introduced. Those key technologies are integrated and realized on the Client Server model.
- To ensure that CIS will be highly reliable system, the use of dual-system server for Main Server at Head Office is recommended.
- To make CIS application a user-friendly system, the application must be built to provide users with Graphical User Interface.
- To secure CIS, the system will implement password to control access and grant users different sets of privileges based on their designations.
- To make system maintenance easy, it is highly recommended to use tools that provide some functions, such as job scheduling, resource distributing, and system monitoring.

3.2 Reliability Design

3.2.1 Circumstances

CIS serves critical business process to DJBC. Generally, higher reliability of computer system is obtained mainly by duplicating its components.

Different levels of reliability for each component, such as the server and the clients, are required in accordance with their role in the system. Major components of CIS are listed in Table 3.1.1.1-2 with descriptions.

The reliability requirements for each component are settled considering several factors.

Below is list of factors that determine reliability of each facility and alternatives for each factor:

- CPU
  - Dual CPU vs. single CPU
  - Multi-processor vs. single processor within one CPU

  For definition of CPU and processor, refer to 3.2.3.
- Power supply
  - Use of un-interruptible power source (hereinafter referred to as UPS) vs. no UPS
  - Duplicated power units within one CPU vs. single power unit
- Disk
  - Use of disk array system vs. ordinary disk units
  - Use of duplicated disk controllers within one CPU vs. single disk controller
- LAN
  - Duplication of transmission line vs. single transmission line
  - Duplication of network facilities vs. single network facility
- WAN
  - Duplication of network services vs. single network service
  - Duplication of network facilities vs. single network facility

Together with above factors, the cost that will be risen by the duplication was also major determinant through the discussion between DJBC and the JICA Study Team.

3.2.2 Reliability scope of CIS

This subsection summarizes the requirement for reliability of components in CIS. Components are classified into the Main Server, Regional Server type I, II and III, and Clients.

Table 3.2.2-1 shows the required configuration for each component:

Table 3.2.2-1: Reliability requirements for components

Facilities	CPU	Power supply	Disk
Main Server	• Dual CPU • Multi-processor	• UPS • Single Power Unit	• Disk array • Dual disk controllers
Regional Server type I	• Single CPU • Multi-processor	• UPS • Single Power Unit	• Disk array • Dual disk controllers
Regional Server type II	• Single CPU • Multi-processor	• UPS • Single Power Unit	• Disk array • Single disk controller
Regional Server type III	• Single CPU • Single processor	• UPS • Single Power Unit	• Disk array • Single disk controller
Clients	• Single CPU • Single processor	• UPS	• Ordinary disk units

Note: For actual configurations, which reflect above requirements, refer to 3.8.

Reliability requirements for networking both within and between offices are shown in the next table:

Table 3.2.2-2: Reliability requirements for networking

Office	LAN within office	WAN connection to Head Office
Head Office	• Single transmission line • Duplicated network facilities	—
Offices in Tj. Priok area	• Single transmission line • Duplicated network facilities	• Duplicated network services • Duplicated network facilities
Other offices	• Single transmission line • Single network facilities	• Single network service • Single network facility

Note: For actual network configuration, refer to 3.7.

Details of each topic are explained in following subsections.

3.2.3 CPU

In CIS, these two terms are used in accordance with DJBC's convention:

- The term "CPU" is defined as a centric unit of computer system that contains processor(s), bus, memory, power supplying unit, and other essential parts of the system.
- The term "processor" is defined as a functional unit that interprets and executes instructions.

Alternatives for configuration of the CPU are as follows:

- Dual CPU vs. single CPU

  Dual CPU configuration consists of primary CPU, backup CPU and multihost disk system.

  Dual CPU configuration guarantee continuing operation with short interruption when one failure occurs on the system. The reason is that a dual CPU configuration has no potential points of failure that can bring whole system down: all the components, i.e. CPU, disk, and interconnections between components, are dualized.

  Figure 3.2.3-1 (next page) shows outline of dual CPU configuration. For detailed configuration of the system, refer to 3.8.2.

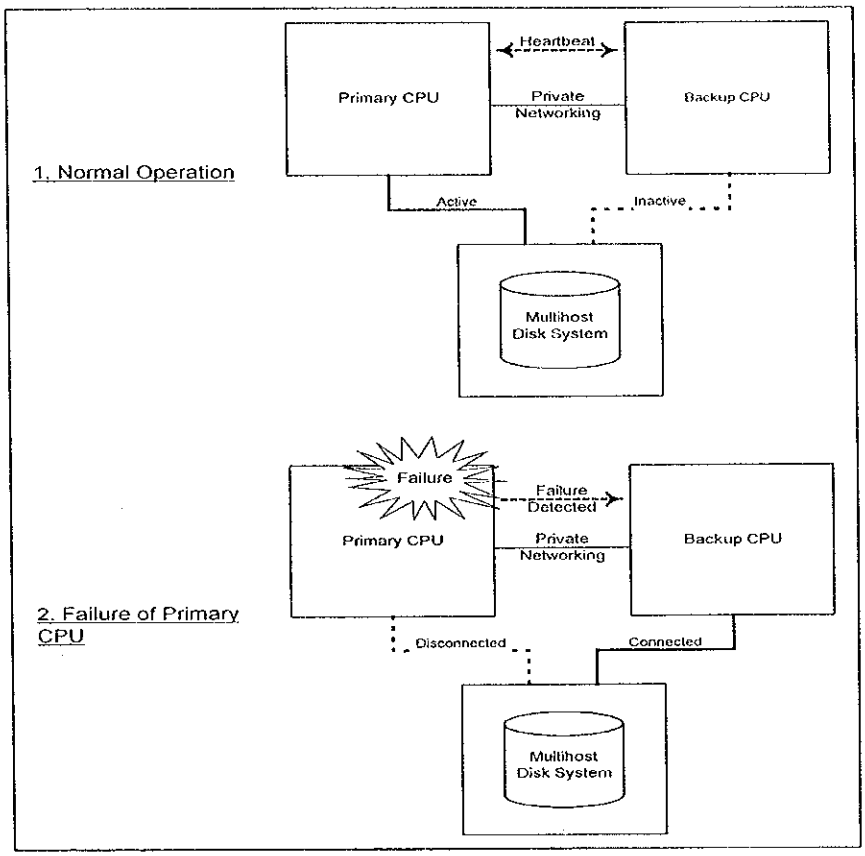

Figure 3.2.3-1: Dual CPU configuration

In normal operation, primary CPU and backup CPU are regularly communicating each other to confirm that they are functioning (this communication is called "heartbeat"). This communication is performed through private networking line. Both of CPU are connecting to multihost disk system, and connection to primary CPU is only active in normal operation.

When primary CPU fails, backup CPU detects the failure and activates connection to multihost disk system. After checking consistency of file system, the backup CPU starts up recovery process of service. Then the backup CPU restarts the service. IP address of primary CPU is taken over by backup CPU.

In single CPU configuration, failures on the CPU cause whole system down. As previously mentioned, CPU consists of processor(s), bus, memory, power supplying unit, and other essential parts of the system.

- Multi processor vs. single processor

  Multi processor configuration should be interpreted to install more than one processor in one CPU.

  Multi processor configuration reduces downtime in case of processor failure as long as there is at least one processor working in the CPU.

  Figure 3.2.3-2 illustrates operation in multi processor configuration.

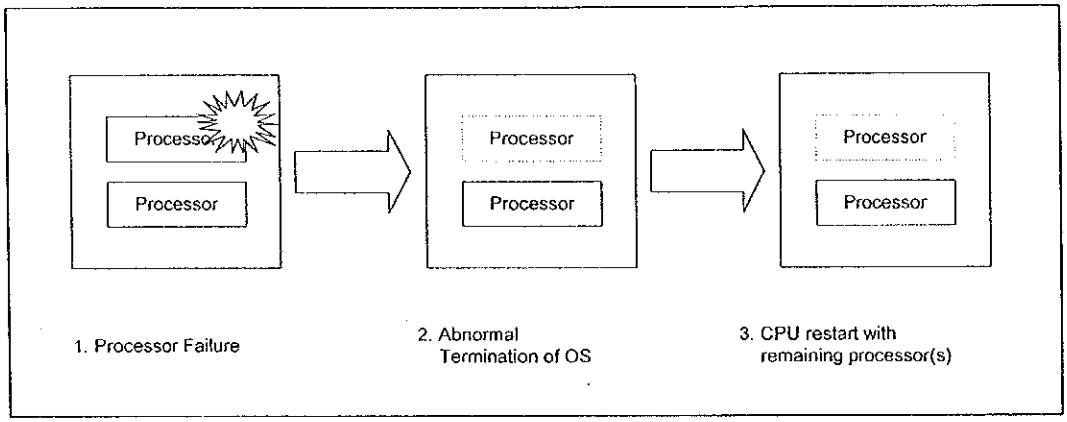

Figure 3.2.3-2: Multi processor configuration

When one processor fails in operation, the OS running in the CPU terminates abnormally. After restarting, the CPU is run by remaining processor(s). Recovery processes are executed at first, then service is resumed.

Contrary, in single processor configuration, failure on the processor causes down of whole CPU until the processor is replaced by new one.

The major difference between dual CPU and multiprocessor configuration is that all the components of CPU are duplicated in dual CPU configuration. On the other hand, multiprocessor system duplicates only processors in CPU. When components other than processor fails, only dual CPU configuration system can resume operation.

Through the discussion between DJBC and the JICA Study Team, dual CPU configuration is required for the CIS Main Server. Single CPU configuration is required for other servers, namely Regional Server Type I, II, and III, and the CIS clients.

One of the reason is that when components in the system fail, sometimes hardware venders take long time to prepare replacements. That interruption of operation is not acceptable for the CIS Main Server because it manages the entire operation of CIS and no other server can take over the business processes. For other components, the doubled hardware cost by duplicating CPU is not preferred.

Multiprocessor configuration is required for the CIS Main Server, Regional Server Type I and II. Single processor configuration is required for Regional Server Type III and the CIS clients. The multiprocessor configuration provides system with higher performance and expandability in addition to higher reliability. The number of processors of each server is in proportion to the amount of estimated data each server processes.

3.2.4 Power Supply

Alternatives for configuration regarding power supply are as follows:

- Dual power units vs. single power unit.
- Installing UPS

Figure 3.2.4-1 shows the general relationship between UPS and CPU.

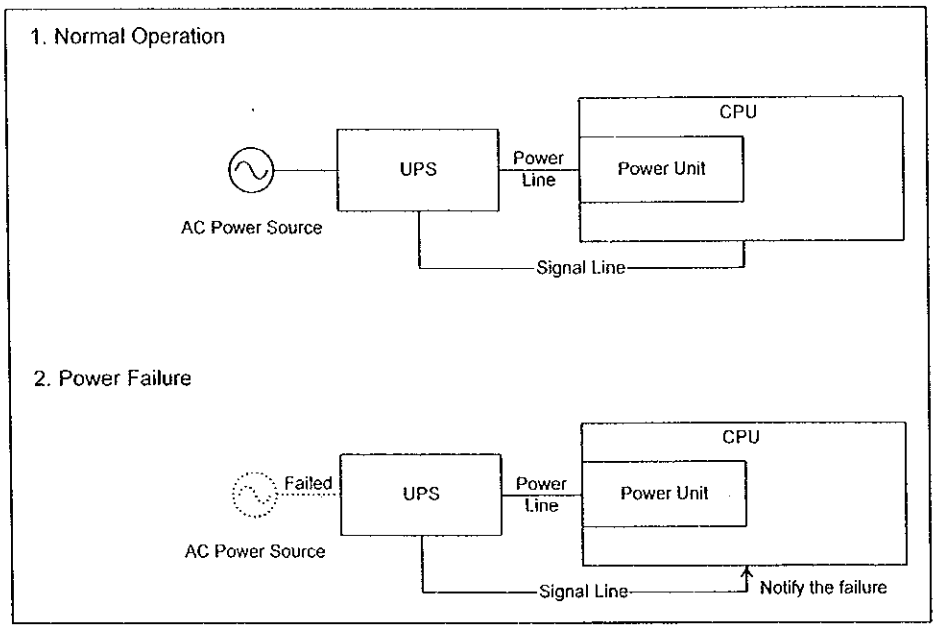

Figure 3.2.4-1: General operation of UPS

Power unit is a component of CPU. Major roles of power unit are to transform voltage and rectify current supplied from AC power source. Duplication of power unit within one CPU guarantees continuous operation if one power unit fails. Contrary, in single power unit configuration, the CPU stops if the power unit fails. The duplicated power unit configuration is possible only for servers.

UPS supplies power for CPU in case AC power source fails. Without UPS, the CPU immediately turns to blackout upon AC failure.

If one UPS is dedicated to one CPU, they are generally connected both power line and signal line. The power is supplied through power line while the conditions of AC power source and UPS itself through signal line. When AC power fails, the UPS notify CPU the incident. The CPU can start shutdown process if the failure continues to run out the battery of the UPS.

Through the discussion between DJBC and the JICA Study Team, dual power unit configuration is not preferred for all components of CIS. The reason is that AC power failure is more likely to happen than power unit failure, so that investment to power unit is not regarded as cost-effective.

UPS will be installed to all the components of CIS instead. The installations for servers differ from those of clients. The Main Server, Regional Server Type I, II and III will have their private UPS. The servers will be connected to their UPS by both power line and signal line. The CIS clients will be connected to central UPS installed in each building of DJBC offices. The clients will be connected through power line only. Therefore, each client cannot detect AC failure and shutdown. DJBC employs this configuration for current computer systems in each office.

3.2.5 Disk

Alternatives for configuration regarding disk are as follows:

- Disk array vs. single disk

  Disk array provides these capabilities to storage system:

  1) Multi-host configuration

     One disk array can be connected to more than one server at the same time. As discussed in 3.2.3, this feature is essential for dual CPU configuration.

  2) Hot swapping of disk unit

     Parts of disk drive units in array system can be swapped without powering off the whole storage system. This enables non-stop operation of the storage system when disk array system is combined with RAID configuration described below.

  3) RAID configuration

     RAID configuration provides redundancy to storage system. Data are stored with additional information that detects error and recovers the original data if parts of them are lost. Thus RAID system can operate even when part of disk unit is failed, but in such case disk failed must be exchanged with new one; the redundancy provided by RAID system, which is essential to guarantee reliability, is lost during the time.

  On the other hand, single disk system configuration does not have capabilities listed above. Each disk unit is connected to one CPU. Data redundancy is not provided by disk system hardware. The advantage of single disk system configuration is its lower cost in comparison with disk array system.

- Dual disk controllers vs. single disk controller in one CPU

  In dual disk controller configuration, each CPU has two disk controllers both of them are connected to disk system. The dual disk controller configuration guarantees continuous operation of one of the controller should be down.

  In single disk controller configuration, failure of the controller makes whole system down.

As the result of discussion between DJBC and the JICA Study Team, disk array system is preferred for all the CIS servers: the CIS Main Server, Regional Server Type I, II and III. The CIS clients equip single disk unit of industrial standard within each CPU.

The CIS Main Server and the Regional Server Type I will have two disk controllers. This is the same configuration with current major computer system in DJBC. Other components, Regional Server Type II, III, and the CIS clients will have one disk controller in each CPU.

Figure 3.2.5-1 illustrates the storage configuration of each CIS component.

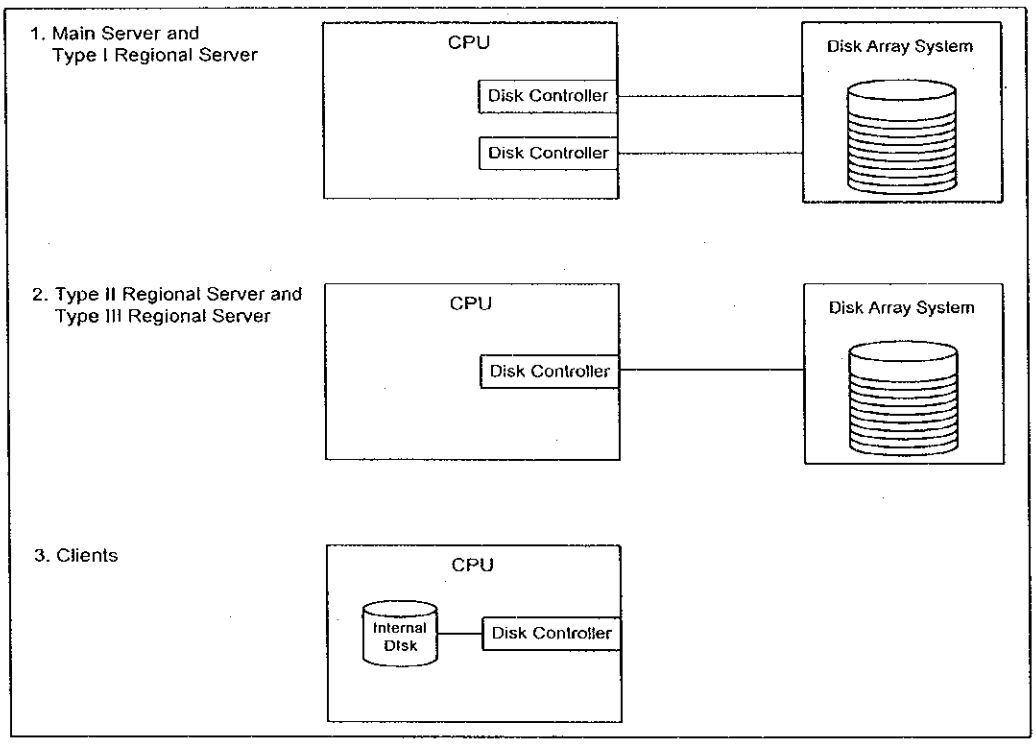

Figure 3.2.5-1: Disk configuration of each component

3.2.6 Network

3.2.6.1 LAN

Alternatives for LAN configuration are as follows:

- Multiple transmission line vs. single line

  In multiple transmission line configuration, every computer has duplicated network adapters, both of which are connecting to network equipment such as hub or router. The two network adapters of each computer have different network addresses and work as primary and backup. This configuration guarantees continuous operation in case primary transmission line fails.

  In single transmission line configuration, each computer is connected to network equipment through single network adapter and transmission line.

- Duplicated network facilities vs. single network facility

  Here the network facility should be interpreted as hub, router, or other controlling equipment of LAN. There is a restriction that more than one network facility cannot play exactly the same role in one network.

  Therefore, the duplication of network facility means preparing two identical network facilities for one networking function: the one for primary use and the other for backup. Naturally, single network facility configuration implies no backup facility at each site.

Through the discussion between DJBC and the JICA Study Team, single transmission line configuration is preferred for the CIS LAN. Multiple transmission line configuration is avoided because of its complexity and lack of cost-efficiency.

For network facilities, centric parts of CIS LAN, such as segment switches, will be duplicated; namely, backup equipment is prepared in the site. In case of failure, the maintenance staff will replace failed parts with backup.

Figure 3.2.6.1-1 (next page) shows the concept of LAN reliability of CIS.

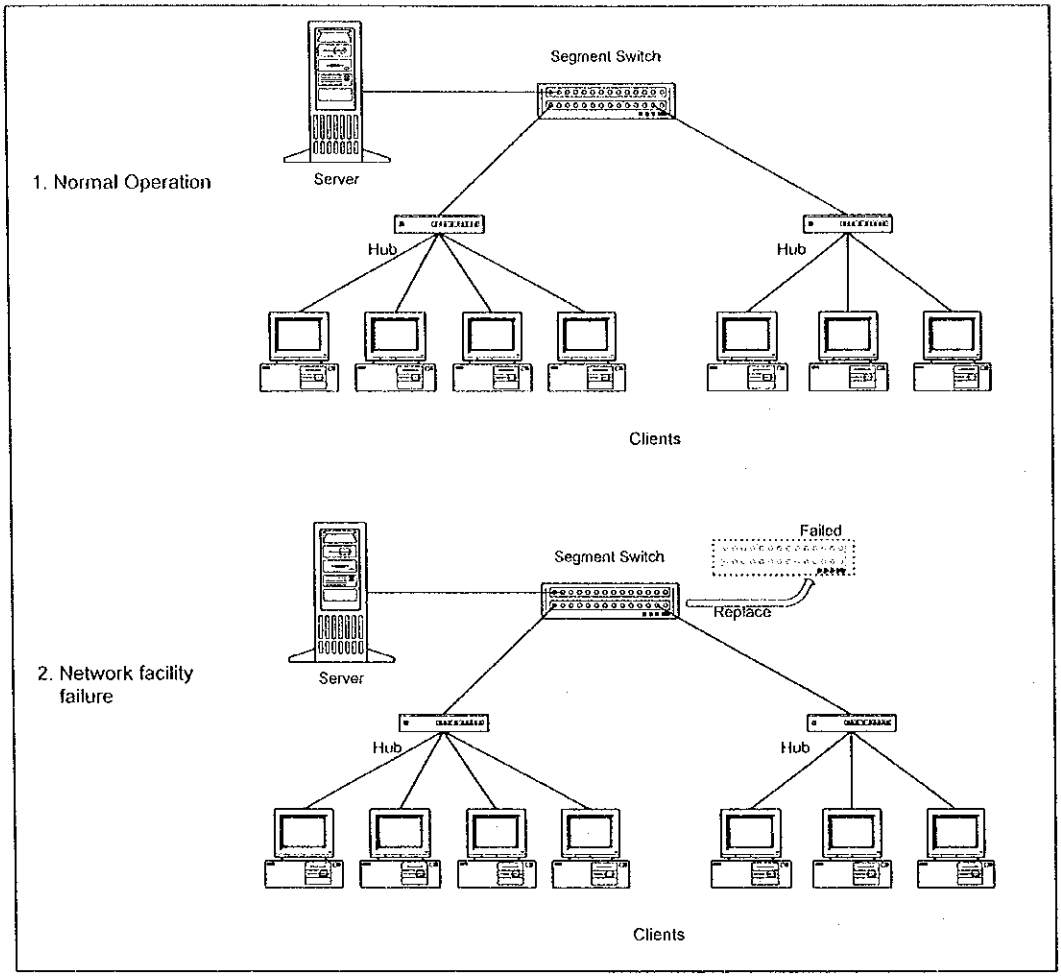

Figure 3.2.6.1-1: Reliability concept of CIS LAN

3.2.6.2 WAN

WAN connects between two or more LANs installed in each office of DJBC. WAN is constructed on the basis of public network services: digital leased line, ISDN, or VSAT.

Alternatives for WAN configuration are as follows:

- Multiple network services vs. single network service

  In multiple network service configurations, more than one different kind of network services (e.g. digital leased line and ISDN) is employed to connect two distant sites: the one service for primary use and the other for backup. If the primary network service stops, the data communication between two sites is switched to backup service.

  On the other hand, only one network service is employed to connect two sites in single network service configuration.

There is restriction that types of available network services depend on the area. For example, digital leased line, ISDN and VSAT are available in Jakarta area while only VSAT is available in provinces.

- Duplicated network facilities vs. single network facility

  Here the network facility should be interpreted as router, modem or other equipment to connect each LAN to public network services. There is a restriction that more than one network facility cannot play exactly the same role in one network.

  Therefore, the duplication of network facility means preparing two identical network facilities for one networking function: the one for primary use and the other for backup. Naturally, single network facility configuration implies no backup facility at each site.

Through the discussion between DJBC and the JICA Study Team, WAN connection of high reliability is required to connect Head Office to offices in Tj. Priok area. The reason is that offices in Tj. Priok area deal with large amount of transactions (about 70% of all the transactions of Indonesia). Multiple network services configuration is required for these connections. For connections from Head Office to other offices of DJBC, which will be implemented in the second and later stage, use of single network service is preferred.

Figure 3.2.6.2-1 (next page) shows the concept of reliability of CIS WAN.

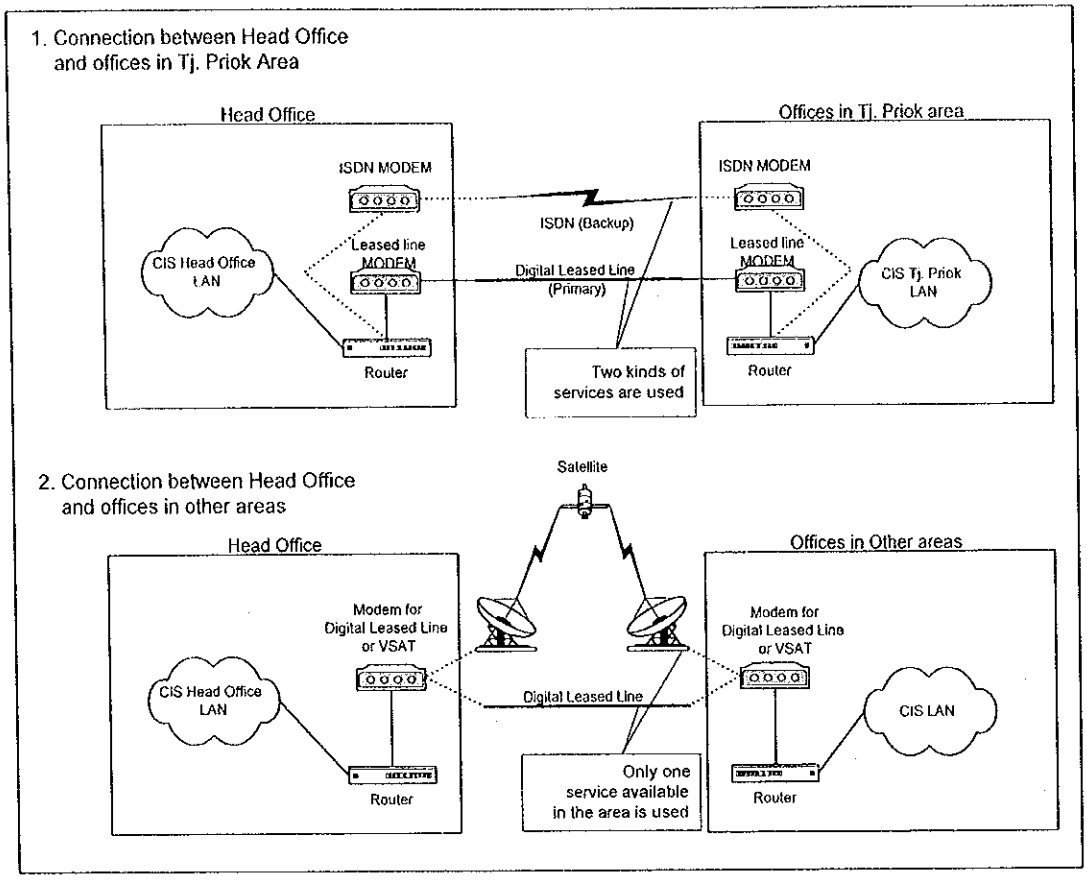

Figure 3.2.6.2-1: Reliability concept of CIS WAN

1) Connection between Head Office and offices in Tj. Priok area

Digital leased line and ISDN will be used in this connection. Leased line is used as primary connection, while ISDN as backup.

In case of leased line failure, routers at both sites detect the failure and automatically switch the connection to ISDN.

2) Connections between Head Office and offices in other areas

The kind of available public network service depends on each area.

One network service is selected for each area to connect to Head Office. No backup services are prepared for these connections.

3.2.7 Countermeasure for system failure

This subsection explains overview of countermeasures taken for different kinds of failure in CIS. Failures are categorized following the components of CIS, namely servers, clients, and network.

For high availability of the whole system, failures on the servers and networks are required:

- To be detected automatically

  Operating control software plays important role in detection of failures. This topic is discussed in 3.5.5.
- Not to have large impact on business processes
- To be recovered quickly

These qualities are not severely required for failures on individual clients. When one client fails, the business operation can be resumed on another client in the same office. Technically, detection and recovery of client failures are restricted by the limited functionality of their OS.

Expected failures on CIS and countermeasures that should be taken for each failure are listed in Table 3.2.7-1.

Table 3.2.7-1: Countermeasures for system failure (1/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Server	Dual CPU configuration	Processor	Processor failure	1) Primary CPU abnormally terminates. 2) Operation is automatically switched to backup CPU. 3) Maintenance staff replaces failed processor. 4) Maintenance staff switches the operation to primary CPU during maintenance period.	SMALL
		Power unit	Power unit failure	1) Primary CPU suddenly turns to blackout. 2) Operation is automatically switched to backup CPU. 3) Maintenance staff replaces failed power unit. 4) Maintenance staff switches the operation to primary CPU during maintenance period.	SMALL
		AC Power supply	Power failure	1) UPS notify the primary and backup CPU of power failure. 2) If power failure continues, primary and backup CPU shut down.	NONE (short term failure) LARGE (long term failure)
		OS	OS crash	1) Primary CPU abnormally terminates. 2) Operation is automatically switched to backup CPU. 3) Maintenance staff restarts the failed CPU 4) Maintenance staff switches the operation to primary CPU during maintenance period.	SMALL

Table 3.2.7-1: Countermeasures for system failure (2/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Server	Single CPU configuration	Processor (multi processor configuration)	Processor failure	1) CPU abnormally terminates. 2) Maintenance staff restarts the CPU. The CPU resumes operation without failed processor. 3) Maintenance staff replaces failed processor during maintenance period.	SMALL
		Processor (single processor configuration)	Processor failure	1) CPU abnormally terminates. 2) Maintenance staff replaces the failed processor. 3) Maintenance staff restarts the CPU.	LARGE
		Power unit	Power unit failure	1) CPU suddenly turns to blackout. 2) Maintenance staff replaces failed power unit. 3) Maintenance staff restart the CPU	LARGE
		AC Power supply	Power failure	1) UPS notify the CPU of power failure 2) If power failure continues, the CPU shut down.	NONE (short term failure) LARGE (long term failure)
		OS	OS crash	1) The CPU abnormally terminates. 2) Maintenance staff restarts the CPU.	MIDDLE
	Common	Disk system	Disk controller failure (dual controller configuration)	1) CPU detects the failure of one controller. CPU notifies failure to operational control server. 2) Disk operation continues on remaining disk controller. 3) Maintenance staff replaces the failed disk controller.	NONE

Table 3.2.7-1: Countermeasures for system failure (3/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Server	Common	Disk System	Disk controller failure (single controller configuration)	1) CPU detects the failure of the controller. CPU notifies failure to operational control server. 2) Disk operation on the CPU stops. 3) Maintenance staff replaces the failed disk controller. 4) Maintenance staff restart the CPU.	LARGE
			File system full	1) The OS detects the file system became full. The OS notifies the incident to operational control server. 2) Disk operations on the file system first slow down, then stop. 3) Maintenance staff creates disk space for the file system.	MIDDLE
			Failure on single disk unit	1) The OS detects the failure. The OS notifies the incident to operational control server. 2) Disk operations on the disk system continue. 3) Maintenance staff replaces the failed disk unit. 4) Disk system automatically re-creates the information of replaced unit.	NONE

Table 3.2.7-1: Countermeasures for system failure (4/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Server	Common	Disk System	Failure on more than one disk unit	1) The OS detects the failure. The OS notifies the incident to operational control server. 2) Disk operations on the file system containing failed disk units stop. 3) Maintenance staff stops the services. 4) Maintenance staff replaces the failed disk units. 5) Maintenance staff recovers the data on the file system from backup media. 6) Maintenance staff restarts the services.	LARGE
		Software	Program product (PP) failure	1) Operator or operational control software detects the failure of program product. 2) Operator or operational control software restarts the product.	MIDDLE
			User program (UP) failure on batch process	1) User program returns the execution status to operational control software. 2) Operational control software starts up the predefined recovery process.	SMALL
			Database failure	1) The database output execution status to log file and terminate. 2) Maintenance staff investigates the causes of the failure and resolves them. 3) Maintenance staff restarts the database.	LARGE

Table 3.2.7-1: Countermeasures for system failure (5/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Clients	Common	Hardware	CPU failure	1) The client CPU down. 2) Maintenance staff replaces the failed parts with new one. 3) Maintenance staff restarts the client.	SMALL (operation can be continued on other clients)
			Disk failure	1) Disk operations fail. 2) Maintenance staff replaces the failed disk with new one. 3) Maintenance staff restarts the client.	
		Software	OS crash	1) The client CPU down. 2) Maintenance staff investigates the cause and resolves them. 3) Maintenance staff restarts the clients.	
			Program product (PP) failure		
			User program (UP) failure		
Network	LAN	Centric facilities of LAN	Facility failure	1) Operational control software detects the failure. 2) Maintenance staff replaces the failed facilities with backup.	MIDDLE
		Other facilities of LAN	Port level failure	1) Operational control software detects the failure. 2) Maintenance staff switches the connection to living port.	SMALL (impact is limited to connected computers)
			Whole facility failure	1) Operational control software detects the failure. 2) Maintenance staff replaces the failed facility with new one.	MIDDLE (impact is limited to connected computers)

Table 3.2.7-1: Countermeasures for system failure (6/6)

Category	Detail	Component	Incident	Event / Countermeasure / Expected Result	Impact on business processes
Network	WAN	Connection between Head Office and Tj. Priok area	Primary network service down	1) Operational control software detects the failure. 2) Network facility automatically switches the connection to backup service. 3) After the recovery, the connection is switched to primary service during maintenance period.	SMALL
		Connection between Head Office and offices not within Tj. Priok area	Network service down	1) Operational control software detects the failure. 2) Operations stop until the network service recovers. 3) After recovery of service, operations resume.	LARGE

3.3 Security Design

3.3.1 Circumstances

CIS serves critical business process to DJBC. This section explains security specifications of CIS from these categories:

- Hardware
- Software
- Data
- The CIS application

3.3.2 Security coverage of CIS

Table 3.3.2-1 shows the overview of security coverage of CIS. Details are discussed in following subsections.

3.3.3 Hardware

The specifications on hardware security are established considering:

1) Special device for recognition of individuals

CIS does not use any hardware devices to identify each operator, such as voice recognition, fingerprint recognition, or ID card system. The identification of operator is implemented as a function of the CIS application software.

2) Management of facility

CIS is installed within the office of DJBC. The management of the CIS facilities, such as servers, disks, or personal computers follows the current management of existing computer systems or other equipment in DJBC. The security of CIS is derived from the security policy of DJBC. Use of burglarproof hardware or other special devices is out of the scope of CIS design.

3) Network

CIS employs both the internal networking facility for LAN and the commercial network service for WAN.

The security for networking is brought from the standard hardware and the commercial network service. The hardware devices for prevention of tapping or network interference are out of the scope of CIS design.

Table 3.3.2-1: Security coverage of CIS (1/2)

Categories	Items	Sub items		Measures in CIS	Remarks
Hardware	Devices for recognition of individuals	• Voice recognition • Fingerprint recognition • ID card system		Not required for the CIS.	To identify each operator is implemented as a function of the CIS application software using ID and password.
	Computer facilities	• CPU • Board • Keyboard • Workstation • PC • Printer • Disk • Server machine		• No additional device for security is required. • Management of facilities follows the policy for management of other existing system in DJBC.	—
	Network	• Communication line • Router • Hub • Modem			—
Software	Operating system	—		Apply latest patches provided from OS vendor.	To mend known security holes and other defects of OS.
		Network services	Name servers	Disable unnecessary network services.	To protect CIS from unauthorized access.
			Password/Key server		—
			NFS		—
			Fingerd		—
			WWW		—
			File transfer		—

Table 3.3.2-1: Security coverage of CIS (2/2)

Categories	Items	Sub Items	Measures in CIS	Remarks
Software	Operating System	User account (server)	• Categorize user accounts • Give proper privilege to each account category	—
		User account (clients)	• No specific user account on the CIS clients	There are no functions in CIS that requires user account on clients.
	Program product	Anti-virus software	Required for the clients of CIS.	To protect from existing virus.
		Other products	Use security policy of the product.	—
	Database	—	—	Refer to 1.8.6.
	User program	—	—	Refer to 3.3.6.
Data	During execution	Data files	Rely on the security of file system.	—
	Backed up/archieved off-line data	Backed up onto some magnetic media (e.g. DLT)	Management of magnetic media follows the security policy of DJBC.	—
	In transit over communication media	Transferring between server-client	—	—
		Transferring between CIS and other system (e.g. CFRS)	Encryption technology.	Refer to 3.9.5.

3.3.4 Software

This section explains specifications on software security. CIS consists of the server machine and the clients. The server runs on the UNIX operating system, while the clients run on the Microsoft Windows.

3.3.4.1 User accounts

Several kinds of user accounts are used in CIS. Figure 3.3.4.1-1 shows the overview of user accounts. Actual places where each information of accounts is stored are not represented in the figure. Instead, this figure shows categories of user account from the operator's point of view.

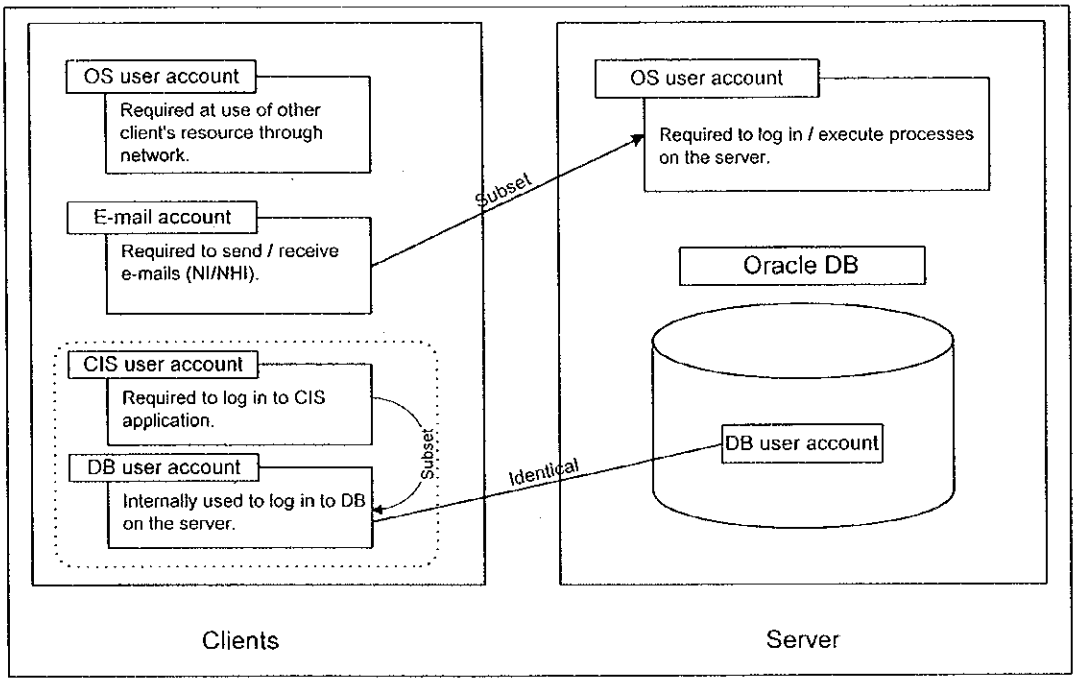

Figure 3.3.4.1-1: Overview of user accounts

Brief description of each type of user account is:

- Client side
  - OS user account

    It is used to log in to each client. If operator needs to access to resource on other clients, input of user account is essential.

    Because there are no such functions required for the CIS clients, OS user accounts for clients are not used in CIS.

- E-mail account

  This type of account is used for sending / receiving e-mail within the CIS network. The purpose of e-mail function in CIS is to exchange NI / NHI information between offices. E-mail account is actually a subset of OS user account on the server, but mainly used for the client.

- The CIS user account

  The CIS user accounts are used at log in to the CIS application. This account determines the user's privilege in CIS according to office that the operator belongs to. The CIS user accounts are a subset of DB user account.

  Detailed explanations of the CIS user accounts are described in 7.1 in Volume III.

- DB user account

  This is identical to DB user account on the server. The CIS clients connect to Oracle DB in the name of certain DB user account at the log-in process of the CIS application.

- Server side
  - OS user account

    This type of user account is required to log in to server / execute processes on the server. Detailed explanations of OS user account on the server are described in 3.7.1.3.

  - DB user account

    DB user account determines the user's privilege in Oracle database on the CIS server. In addition to the CIS user accounts, DB user account includes database system manager account and other special user accounts.

    Detailed explanations of DB user accounts are described in 1.7.1.

3.3.4.2 Operating system

The requirements on security of operating system (OS) are established considering:

1) Security holes of OS

   OS vendors constantly collect the information regarding security holes and other failures of their OS, and release modification modules (patches). Applying latest patches protect the server from the known security holes and faults. For Microsoft Windows, these patches are called Service Pack.

2) Network services

   This topic is applied to the server. Server runs on UNIX OS that provides several functions regarding networking function called network services, including DNS, fingerd, FTP, TFTP, NFS, NIS (+), and others. Most of these network services are not used in CIS. In addition, these network services may allow attack (intentional violation) through network.

Disabling unnecessary network services prevents attacks. Security means for few network services used in CIS, such as FTP and TELNET, accomplished by management of accounts and their privileges.

3) Account management

This topic concerns the server. Every resource in the server, such as files, executing processes, devices and so forth, is logically owned by specific user. The privileges to access resources on the server are granted to each user as a unit. Management of user accounts plays fundamental role in the security of server. For detailed discussion of account management on the server, refer to 3.7.1.3.

3.3.4.3 Program product

- Anti-virus software

  The computer viruses (programs developed to damage the system intentionally) spread among the computers through network or off-line media. To prevent the infection of virus and to detect/remove the viruses from contaminated computers, installation of anti-virus software is required for the clients of CIS.

  The server has little possibility to suffer from viruses for these reasons:

  - OS of the server is secure enough on the condition that the user accounts and privileges are managed properly.
  - Most of computer viruses are written for the personal computers.

- Other products

  The security of program products installed in CIS follows each security policy of the product. For the security means that product provide with, these should be configured to improve the security.

3.3.4.4 Database

For discussion of database security, refer to 1.7.1.

3.3.4.5 User program

For discussion of user program security, refer to 3.3.6.

3.3.5 Data

The requirements on security of data in CIS are established considering:

- Data during execution

  This kind of data is equivalent todata files in the server. The security of the file system of the server is discussed in 3.3.4.1.

- Data archived off-line / backed up

  This kind of data is backed up onto some magnetic media (e.g. DLT). The handling of the media follows the treatment of hardware itself (refer to 3.3.3). The security of this kind of data is brought from the security policy of DJBC.

- Data in transit over communication media

  This kind of data includes the data transferred between the server and the clients, and the data transferred between CIS and other systems (e.g. CFRS). The security of data transferred between CIS and other systems is in 3.9.5.

3.3.6 CIS application

3.3.6.1 User ID and Password check

- The ID-number and the password control user access rights. It is not operating system level password, and it is a separated password system implemented in CIS.
- Anyone who wants to access to CIS has to input his/her ID and Password to validate their rights to access to CIS (refer to Figure 3.3.6.1-1). CIS security-function will check ID and Password in "Table of the CIS Security Data" that is maintained by ADP staff. Once ID and Password are confirmed, CIS security function will not check ID and Password any more.

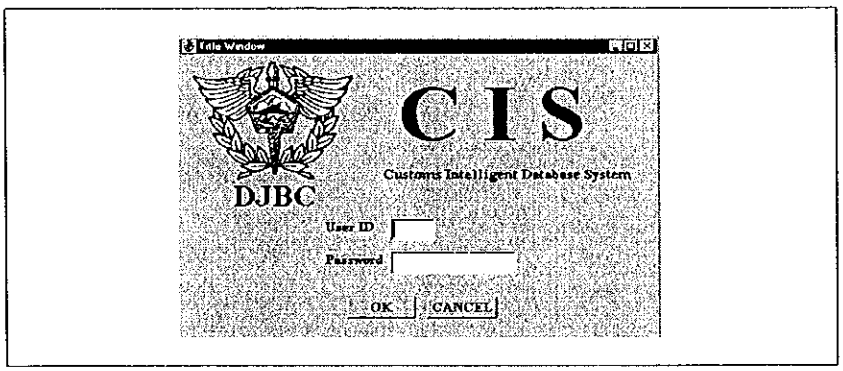

Figure 3.3.6.1-1: Title Window

- One directorate will have limited access rights to information owned by other directorates. The User ID will be related to directorates and sub directorates. That same ID will control the top menu of functions available to the user.
- Within the same directorate, every ID / Password has an equal access level.
- Refer to 7.1 in Volume III for details.

3.3.6.2 Restriction in application menu

The available applications are different depend on inputted User ID.

3.3.6.3 Setting up authority of updating process

The directorates that able to update information will be specified by setting management authority to that information.

3.3.6.4 Display restriction in Monitor applications

All users (all Directorate, Regional Offices and Service Offices) are basically able to use retrieval related processes, but some information will not display.

3.3.6.5 Security when leaving computer

A Screen Server Function with a password protection will operate if the computer is untouched for certain period of time.

3.4 Performance Design

3.4.1 Circumstances

1) Transaction estimation

Generally, the number of transaction would have to be investigated to define the scale of the hardware and network speed.

This section describes how to estimate the number of transaction in CIS and which points are considered in the estimation. It is not easy for both JICA Study Team and end users to estimate the number of transactions in CIS. Because most of the business operations in CIS will be created newly and end users cannot perceive how often they will access to CIS. Despite the difficulties, the JICA Study Team estimated the transaction number in CIS as follows.

- Estimating the number of business operation transactions per day in each function of First stage. This means the number of end user accessing CIS.
- Estimating the system access transaction number per day in each function of First stage. This means the number of actual accesses to CIS.
- Considering possibility of increasing numbers of transactions.
- Estimating the peak actual transaction number.
- Estimating the peak number in each location, such as Head Office and Regional offices, in second and later stages.
- Estimating the peak number and capacity of Network (in Detail Design).

2) Wide area network speed estimation

Estimating the network speed, especially Wide Area Network speed is one of the most important factors to realize the connection among the customs offices. In addition, it would affect the operational cost and the response time in the CIS function, such as online process function and file transfer function. In this subsection, the JICA Study Team has estimated the throughput of file transferring through WAN and the throughput time of the online process through WAN.

3) Performance checkpoints

In client-server computing system on open platform, however, precise behavior of system is not calculated on paper estimation. CIS belongs to this kind of system.

Instead, testing performance on actual computer system is needed to predict performance of CIS. Basic idea here is to develop prototype system and to measure the performance of the

prototype. The means for performance specification of CIS must be reconsidered based on the result of the test.

This sub-subsection describes the basic procedures and checkpoints on the test.

3.4.2 Estimation grounds

3.4.2.1 Transaction estimation

1) Estimating the number of business operation transaction in first stage.

The estimated number of business operation transactions in each CIS function of first stage is shown in Table 3.4.2.1-1. That number is based on the results of hearing at each directorate on November 1998. The estimation is based on the assumptions following the information gathered during Basic Investigation phase. Some of the assumptions include investigated number of PIB, PEB and other current existing data, while others come from Japanese CIS case. However, CIS is the first operation in Indonesian Customs, and it is most certain that the condition is different from the Japanese CIS and the needs of Customs operations of CIS might change after starting the CIS operations.

Another point to note is that in each development stage of CIS, the increase in the number of transactions must be re-estimated according to the CIS requirements and functions. The increase in the number of transactions may differ from the original estimation, because the integrated database would be very useful and it would provide the additional instrument for customs operation. Moreover, DJBC has a plan to expand CIS to the Customs National Database, which would be the concept of multipurpose database systems concept of Indonesia customs.

2) Estimating the system access transaction number in first stage

Each business transaction of an application program usually consists of internal accesses, which are actual system accesses to the server from the client computer. The assumption made is that each transaction that updates the data, such as registration, update, and delete transactions, has 10 internal accesses. Monitoring data business transaction, such as retrieving transactions, has 5 internal accesses. Therefore, considering the above conditions, the system access of transactions (internal accesses) are expected to be approximately 222,000 transactions per day (refer to Table 3.4.2.1-1).

3) Possibility of increase in transaction per day

In this report, the main source for the increase in the number of transactions in CIS is assumed to be the increasing number of business transaction of Import and Export, which is estimated at the rate of approximately 5.0% per year. Therefore, the CIS transactions increase rate is also assumed 6.0% with adding 1% risk rate

The number of transactions in 5 years is increased at approximately 26% of originally estimated business transactions.

4) Estimating the peak system transaction number in first stage

In this report, the peak system transaction is the number of transaction at peak time that the system needs to handle. The number is assumed 50% of total daily transactions by an hour. Therefore, the peak system transaction would be approximately 2,340 Transactions per Minute (hereinafter referred to as tpm). For more details, refer to Table 3.4.2.1-1.

5) Estimating allocation of transaction in each server and each stage

The JICA Study Team has assumed the following conditions in order to estimate the peak transaction in each server machine, such as Main Server and Regional Server.

- The peak transaction of the first stage in Main Server is regarded as the base (100%).
- Total peak transaction at the second and later stages is 250% of the peak transaction of the first stage. The increase is due to additional functions and additional regional servers and terminals.
- Half of the total peak transaction at the second and later stage is handled by the Main Server and the other half is divided among the Regional Servers.

Therefore, at second and later stages, the peak transaction of the Main Server is estimated at 125 % of the peak transaction in the first stage. The total peak transaction in Regional Servers at second and later stages is also estimated at 125%. The number of transactions is divided among the Regional Servers. For the ratio of the number of transactions among each of the Regional Server, refer to Table 3.4.2.1-2.

These conditions, however, must be re-analyzed during each development phase.

Table 3.4.2.1-1: Estimated number of transactions in the CIS first stage (1/4)

No.	Site	Department / Section	Application Name	Transaction				
				Register	Update	Delete	Retrieval	Total
C-1 (0-1)	Client Job Processing	Common	User ID, Password Check	0	0	0	4,000	4,000
C-2 (0-2)			Job Menu	0	0	0	4,000	4,000
C-3 (0-3)			Change Password	0	12	0	0	12
C-4 (3-7)			PIB Monitor	0	0	0	109	109
C-5 (3-8)			PEB Monitor	0	0	0	109	109
C-6 (3-15)			Summarized importer / exporter information	0	0	0	109	109
V-1 (1-1)		Verification & Audit	PIB Verification Management	2,500	50	25	0	2,575
V-2 (1-2)			PIB Verification Monitor	0	0	0	2,609	2,609
V-7 (1-7)			~~Excise Verification Management~~	~~0~~	~~0~~	~~0~~	~~0~~	—
V-8 (1-8)			~~Excise Verification Monitor~~	~~0~~	~~0~~	~~0~~	~~0~~	—
V-9 (1-9)			Audit Management	900	900	10	0	1,810
V-10 (1-10)			Audit Monitor	0	0	0	1,115	1,115
P-3 (2-5)		Prevention and Investigation	~~Manifest Management~~	~~0~~	~~0~~	~~0~~	~~0~~	—
P-4 (2-6)			~~Manifest Monitor~~	~~0~~	~~0~~	~~0~~	~~0~~	—
P-7 (2-9)			NI/NHI Management	40	40	40	0	120
P-8 (2-10)			NI/NHI Monitor	0	0	0	40	40
P-9 (2-11)			Violation Management	125	125	125	0	375
P-10 (2-12)			Violation Monitor	0	0	0	139	139
P-13 (2-15)			~~Risk Indicator Management~~	~~0~~	~~0~~	~~0~~	~~0~~	—
P-14 (2-16)			~~Risk Indicator Monitor~~	~~0~~	~~0~~	~~0~~	~~0~~	—
P-15 (2-17)			Past record and blocked importer Management	10	10	10	0	30

Table 3.4.2.1-1: Estimated number of transactions in the CIS first stage (2/4)

No.	Site	Department / Section	Application Name	Transaction				
				Register	Update	Delete	Retrieval	Total
P-16 (2-18)	Client Job Processing	Prevention and Investigation	Past record and blocked importer Monitor	0	0	0	100	100
P-19 (2-21)			Company profile Management	100	100	100	0	300
P-20 (2-22)			Company profile Monitor	0	0	0	186	186
P-27 (2-29)			Inter Island transportation Management	25	25	25	0	75
P-28 (2-30)			Inter Island transportation Monitor	0	0	0	25	25
P-49 (2-51)			Passenger & border crosser Management	25	25	25	0	75
P-50 (2-52)			Passenger & border crosser Monitor	0	0	0	40	40
P-51 (3-13)			Physical examination result Management	200	200	200	0	600
P-52 (3-14)			Physical examination result Monitor	0	0	0	206	206
F-1 (3-3)		Customs Facilitation	Bonded storage Management	20	20	0	0	40
F-2 (3-4)			Bonded storage Monitor	0	0	0	71	71

Table 3.4.2.1-1: Estimated number of transactions in the CIS first stage (3/4)

No.	Site	Department / Section	Application Name	Transaction				
				Register	Update	Delete	Retrieval	Total
T-1 (3-5)	Client Job Processing	Customs Technique	Temporary Admission Management	40	40	0	0	80
T-2 (3-6)			Temporary Admission Monitor	0	0	0	130	130
T-7			~~Temporary Storage Management~~	~~0~~	~~0~~	~~0~~	~~0~~	—
T-8			~~Temporary Storage Monitor~~	~~0~~	~~0~~	~~0~~	~~0~~	—
R-2 (4-6)		Revenue Planning	Revenue data collection for EUC (Excise revenue)	0	0	0	20	20
R-4 (4-3)			PIB data collection for EUC	0	0	0	20	20
R-5 (4-4)			PEB data collection for EUC	0	0	0	20	20
E-3 (4-7)		Excise	Excise company Management	10	150	3	0	163
E-4 (4-8)			Excise company Monitor	0	0	0	40	40
S-1 (A-1)	Server Job Processing	Common	Registration, Change and Deletion of User Information	200	200	200	0	600
S-3 (B-1)			Registration of Information on Import Declaration	2,000	400	0	0	2,400
S-4 (B-2)			Registration of Information on Export Declaration	2,000	400	0	0	2,400
S-5 (C-1)			Creating Profile of Suspicious Importers	2,000	0	0	0	2,000
S-9 (D-4)			Initial Transfer Process	2,000	0	0	0	2,000
I.			Sub-total of transaction [/day]	12,195	2,697	763	13,088	28,743

Table 3.4.2.1-1: Estimated number of transactions in the CIS first stage (4/4)

No.	Transaction	Number of Transactions				
		Register	Update	Delete	Retrieval	Total
I.	Sub-total of transaction [/day]	12,195	2,697	763	13,088	28,743
II.	System access transaction [/day]	121,950	26,970	7,630	65,440	221,990
III.	Increasing of transaction in five years(6% per year) [/day]	153,959	34,049	9,633	82,616	280,257
IV.	Peak system access transaction [/hr]	—	—	—	—	140,129
V.	Peak system access transaction [/min]	—	—	—	—	2,335

Table 3.4.2.1-2: TPM and ratio of TPM in each server

Stage	Main server	Regional server
1st stage	100% [2,340 tpm]	None
2nd and later stages	125% [2,925 tpm]	Total transaction in Regional Offices 125% [2,925tpm] Jakarta IV 85% [1,989 tpm] Surabaya 15% [351 tpm] Bandung 15% [351 tpm] Other 9 Regional Offices 10% [234 tpm]

Note: Regional Office transaction ratios are roughly based on the current PEB/PIB proportion.

Therefore, each server machine must be configured to be able to handle the above transactions per minute during peak times. However, further investigation would be needed regarding the number of transactions.

3.4.2.2 Wide Area Network speed estimation

1) Throughput of file transferring through WAN

According to the result of hearing, approximately 2,000 PIB /day and 2,000 PEB /day would be submitted at Service Offices, and those data are to be transferred from Service Offices to Head Office. In Tanjung Priok area, Service Office 1, Service office 2 and Service Office 3 would directly transmit those data to Head office everyday. To simplify the calculation, the size of each record is supposed to be approximately 2.0 Kbyte. Total daily size of file to be transferred in a day is to be maximum 8.0 Mbyte.

Tanjung Priok Service Office 1, Service Office 2 and Service Office 3 are assumed to transmit the 2.0 Mbyte of data to Head Office, respectively. Other Service Offices are assumed to transmit the 0.5 Mbyte of data to Head Office, respectively. Therefore, the WAN throughput would be estimated in Table 3.4.2.2-1. According to the estimating the throughput of file transfer, 256 Kbps speed seems to be enough for daily data to be transmitted to Head Office. Each office in Tanjung Priok can transmit their daily data to Head Office within several minutes. On the other hand, 64 Kbps may be enough for data to be transmitted from other Service Offices to Head office.

2) Throughput of online process through WAN

Total throughput usually consists of the terminal process throughput, the network transmitting throughput and server process throughput. In this sub-subsection, the JICA Study Team has tried to estimate the network transmitting throughput of on-line through WAN.

The JICA Study team has estimated the following two cases as examples. The case I is supposed to be one of the worst cases. All CIS terminal in each Service Office or Regional Office always access the CIS Main Server to get 50 records of data at the same time. In the case of 256 Kbps network speed, the network throughput of each terminal would take from approximately 30 seconds up to several minutes (refer to Table 3.4.2.2-2).

The case II might be one of the relatively optimistic cases. All personal computers in each Service Office or Regional Office access CIS Main Server to get one record of data at the same time. In the case of 256 Kbps network speed, it would take around a second for the network to transmit throughput in each terminal (refer to Table 3.4.2.2-3). In the case II, there would not be any problem in WAN throughput, however, if end users are always accessing more than 50 records at the same time, WAN throughput would become very slow.

According to these estimations, such as the WAN throughput of file transfer and the WAN throughput of online process, and the cost effective speed of network, at least 256 Kbps speed should be needed for WAN between Tanjung Priok area and Head Office. However, if CIS terminals are always used under the condition of the worst case, such as the case I, or if DJBC wants quicker response in the CIS functions, the speed of WAN should be upgraded up to 512 Kbps or more in Tanjung Priok area. Considering the current network infrastructure situation, the speed of 512 Kbps must be expensive and network service may be unstable in Indonesia. The JICA Study Team would like to suggest that DJBC consider the usage of CIS, and evaluate the network speed and its cost in the later stage again.

Table 3.4.2.2-1: WAN throughput of file transfer

Location	Daily transfer size of file (MB)	Daily transfer size of file (Kbit)	Network speed (Kbps)	WAN throughput (Sec)
Tanjung Priok Service Office 1	2.0	16,777	256	93.6
Tanjung Priok Service Office 2	2.0	16,777	256	93.6
Tanjung Priok Service Office 3	2.0	16,777	256	93.6
Other Servide Offices	0.5	4,194	64	93.6

Note: Network efficiency is assumed 70% in this calculation.

Table 3.4.2.2-2: WAN throughput of on-line process (Case I: 50 records retrieved by all PCs in each office)

Location	Concurrent PC accessing	Records / tran. / PC	The size of transmitting (Kbyte)	Network speed (Kbps)	WAN throughput (Sec)
Tanjung Priok Service Office 1	8	50	800	256	36.6
Tanjung Priok Service Office 2	10	50	1,000	256	45.7
Tanjung Priok Service Office 3	8	50	800	256	36.6
Regional Office	14	50	1,400	256	64.0
Other Service Office	3	50	300	128	27.4

Note: One record is supposed to be 2 Kbyte length.
Network efficiency is assumed to be 70% in this calculation.

Table 3.4.2.2-3: WAN throughput of on-line process (Case II: 1 record retrieved by all PCs in each office)

Location	Concurrent PC accessing	Records / tran. / PC	The size of transmitting (Kbyte)	Network speed (Kbps)	WAN throughput (Sec)
Tanjung Priok Service Office 1	8	1	16	256	0.7
Tanjung Priok Service Office 2	10	1	20	256	0.9
Tanjung Priok Service Office 3	8	1	16	256	0.7
Regional Office	14	1	28	256	1.3
Other Service Office	3	1	6	128	0.5

Note: One record is supposed to be 2kbyte length.
Network efficiency is assumed 70% in this calculation.

3.4.3 Performance checkpoints

3.4.3.1 Overview

This subsection describes outline of performance test design.
The objective of the performance test discussed here is the test that should be performed before starting actual production of CIS.

One method to estimate performance of computer system is to develop detailed model of the system behavior and predict total performance of that system. The examples of values required to calculate performance are:

- The time each client spends to process user request
- Timing of establishing connection between clients and server
- Size of packet transmitted through network in one transaction
- Response time of the database on the server to process request from clients

In client-server computing system on open platform, however, precise values of these variables are not calculated on paper estimation. CIS belongs to this kind of system.
Instead, testing performance on actual computer system is needed to predict performance of CIS. In this case, the test is not necessary to produce values in minute details listed above because the total performance itself is measured directly. The means for performance specification of CIS must be reconsidered based on the result of the test.
The performance of actual CIS should be tested after production. The test should be involved in the product test phase. For the entire plan of the test, refer to 4.2.

Basic idea of this test is to develop prototype system and to measure the performance of the prototype. Performance of system is measured by these two indexes:

- Response time

  Response time is the elapsed time between the end of an inquiry on a system and the beginning of response. Mainly used to indicate performance of online processes.

- Throughput

  Throughput is a measure of the amount of work performed by a system over a period of time. Mainly used to indicate performance of batch processes.

3.4.3.2 Environment for performance test

Followings are guidelines to prepare environments of performance test:

1) Hardware

- Prepare the same type of server with the target CIS Main Server. Different configuration is acceptable except OS and model of processor(s).
- Install actual peripherals on the server. Peripherals include disk storage, tape devices, and network adapters.
- Prepare proper number of client PCs. The same number with the first stage of CIS is not required, but enough number to observe the effect of increasing PCs is required.

2) Software

- Prototype of client application developed by Developer/2000 is required. This must simulate typical CIS applications. The two ways to develop this prototype are:
  - i) Pick up some parts of actual applications if that part is developed on schedule or in advance of it.
  - ii) Develop a small application that includes typical operation of the CIS application.
- Prototypes of batch processes on the server are required. They should simulate typical batch processes on the CIS server.
- Configuring actual database on the server is required. Prototype of stored procedures used by the CIS application must be included.
- Actual size of data. Dummy contents are acceptable but amounts must be identical with the estimated data amount of CIS.

3) Network

- LAN and WAN networking within test environment is required. For WAN configuration, using two network facilities connecting public WAN service is necessary to simulate WAN connection between distant offices.

Proposes of configuration of development environment are found in other part of this report. Section 3.7 explains networking of development as a part of it, and configurations of facilities are found in 3.8.

3.4.3.3 Online processes

Major indexes for online processes are their response time to the operator. Discussion of guidelines for online process design is described in 3.9.1.

Figure 3.4.3.3-1 shows the outline of performance model of online processes.

Response time of online process is determined by elapsed time in client computer, network, and server.

To obtain fundamental data of response time, performance should be measured under controlling following variables:

- Number of client machines connected

  This varies the load of network and server.

- Number of processed record at one transaction

  This varies the load of each client, network, and server. This variable is controlled by retrieving different number of records from one table in the server.

- Networking device (LAN vs. WAN)

  This determines networking capacity between clients and the server. LAN is much faster than WAN. Among popularly used networking devices, for example 10Mbps LAN vs. 64Kbps WAN, the former is over 150 times faster than the latter.

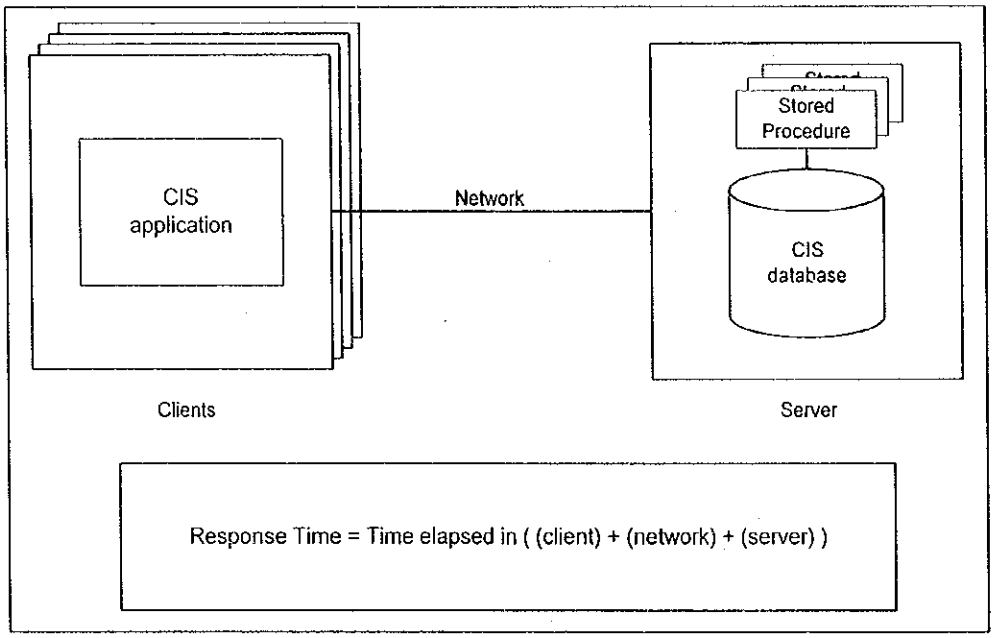

Figure 3.4.3.3-1: Performance model of online processes

The next table shows concept of conditions to measure response. The number of each variable in the table is given as example. The actual number should be reconsidered at the testing.

Table 3.4.3.3-1: Example of performance test conditions

Networking	# of retrieved records	Number of Clients			
		1	5	10	20
LAN	1				
	50				
	100				
	200				
WAN	1				
	50				
	100				
	200				

The indexes of response should be:

- Response time on each client.
- Network load
- Usage of CPU, memory and peripherals on the server

This test will provide basic information regarding response time of online processes of CIS. If the result is not satisfiable, these measures should be taken into account in designing CIS architecture:

- CIS application
  - Expression of SQL

    If SQL used in the prototype is automatically generated by Developer/2000, check the efficiency of the SQL. If they are not proper code, rewriting SQL by following coding standard of SQL is required. The coding standard will be provided before the production stage.
  - Restriction of query pattern

    The flexibility of query to database and the response time are in the trade-off relationship. If response time is of higher priority, restriction of query pattern is required. For example, arbitrary keys to retrieve records should be prohibited.
- Network
  - Employing higher speed network

    The test result provides reliable estimation basis of actual CIS performance. If the planned networking design does not provide enough performance, higher speed networking should be introduced.

- Server configuration
  - Database tuning

    Tuning of parameters of Oracle database used in CIS is both possible in various features and essential. The default values of Oracle database parameters do not provide enough performance in most system.
  - Increasing server capacity

    After tuning components, if the CPU usage or other index on the server predicts lack of server capacity of CIS server, adding CPUs, memory, or peripherals into CIS server configuration should be required.

3.4.3.4 Batch processes

Major index for batch processes is their throughput. All the batch processes of CIS should finish within a half of offline operating period. Detailed explanation of batch processes is described in 3.9.2.

Batch processes are classified into these four categories:

1) Intersystem communication processes
2) Update processes
3) Referential processes
4) Database management processes

Figure 3.4.3.4-1 shows the components relating to each category of batch processes.

The performance of batch processes should be measured by executing the series of batch processes from operational control software.

The major variable to be controlled at the performance test is the amount of data to be processed. In testing intersystem communication processes, testing on different networking devices (LAN and WAN) should be performed in addition.

The elapsed time by each process should be measured. Then throughput of the process is calculated by dividing the amount of data by the elapsed time. Actual processing time in CIS is estimated on throughput and estimated amount of data for each process.

If the processing time does not satisfy the requirement (all the batch process should be executed within a half of offline operation period), the bottleneck of system should be investigated using indicators such as the usage of CPU, memory, and peripherals. The configuration of CIS should be modified to remove the bottleneck.

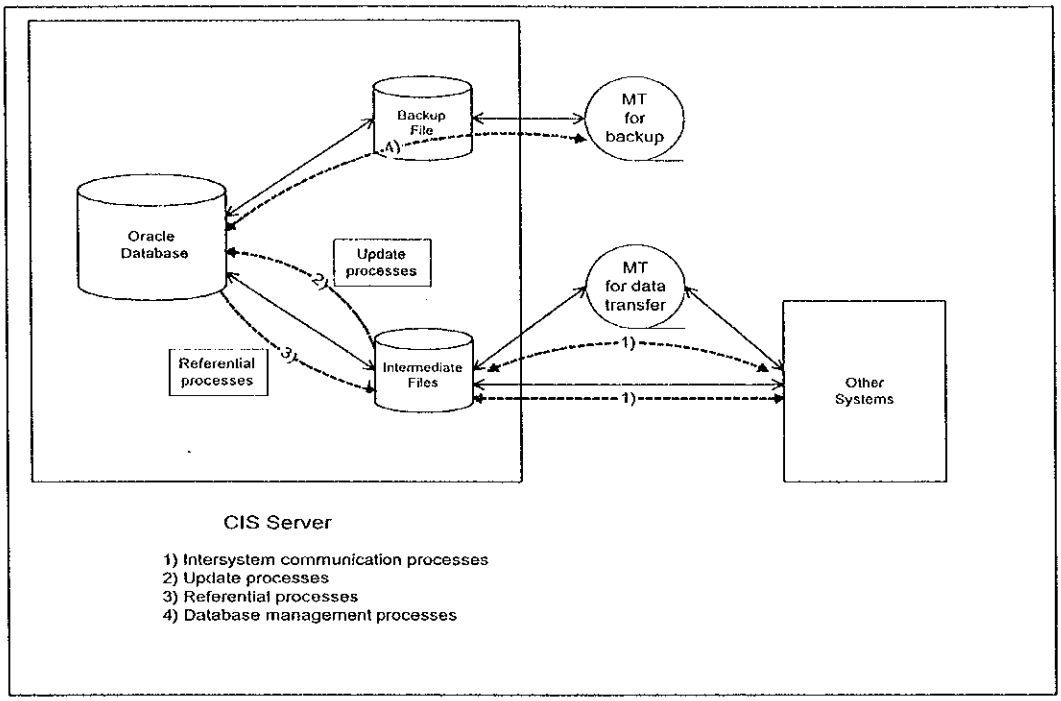

Figure 3.4.3.4-1: Objectives of performance test of batch processes

3.5 Operation Design

3.5.1 Circumstances

CIS will cover DJBC offices distributed to wide regions of Indonesia. Activities of CIS should be monitored and controlled by Head Office. Integrated operation management system is required to keep CIS working and reduce management cost.

This section describes basic operation design of CIS by these categories:

- Overview

  Outline of CIS operation system and explanations of its components are given.
- Operational organizations

  Examples of operating hours, work shifts, and operational rosters are shown.
- Backup

  Backup policy of system components is explained.
- System monitoring

  Monitoring target and method is discussed.
- Resource distribution

  Distribution object and method is discussed.
- Job Management

  Management method of routine jobs is explained.

3.5.2 Overview

One server, which is called operational control server, manages CIS. This server does not perform business operations of CIS; therefore end users do not need to be aware of the machine.

Figure 3.5.2-1 shows the outline of CIS operation system. CIS is installed in Head Office and offices in Tj. Priok area at the first stage.

Followings are operational components of CIS:

- Operational control server

  This is central component of CIS operation. Operating control software package running on this machine enables various functions, such as monitoring activities, scheduling jobs, or resource distribution.

- CIS Main Server

  This server performs CIS business operation. The CIS database is running on this machine. Client component of operational control software is also running on this server, which communicates with its server component on operational control server.

- Model PC

  This is a template of client PCs in CIS. User developed software for CIS client is stored on this machine.

  When the software is revised, the differential package for resource distribution is created on this machine.

- Network facilities (switch, router, hub, and so on)

  These components support CIS networking. Functions of diagnosing themselves and gathering statistical information of network are implemented as standard protocol.

- Clients

  Users operate CIS through these clients.

Operational control server, CIS Main Server, Model PC, and centric network facilities are installed and managed in PUSLATASI. All the clients are installed in each users' office.

In the second and later stages, Regional Servers will be managed by the operational control server.

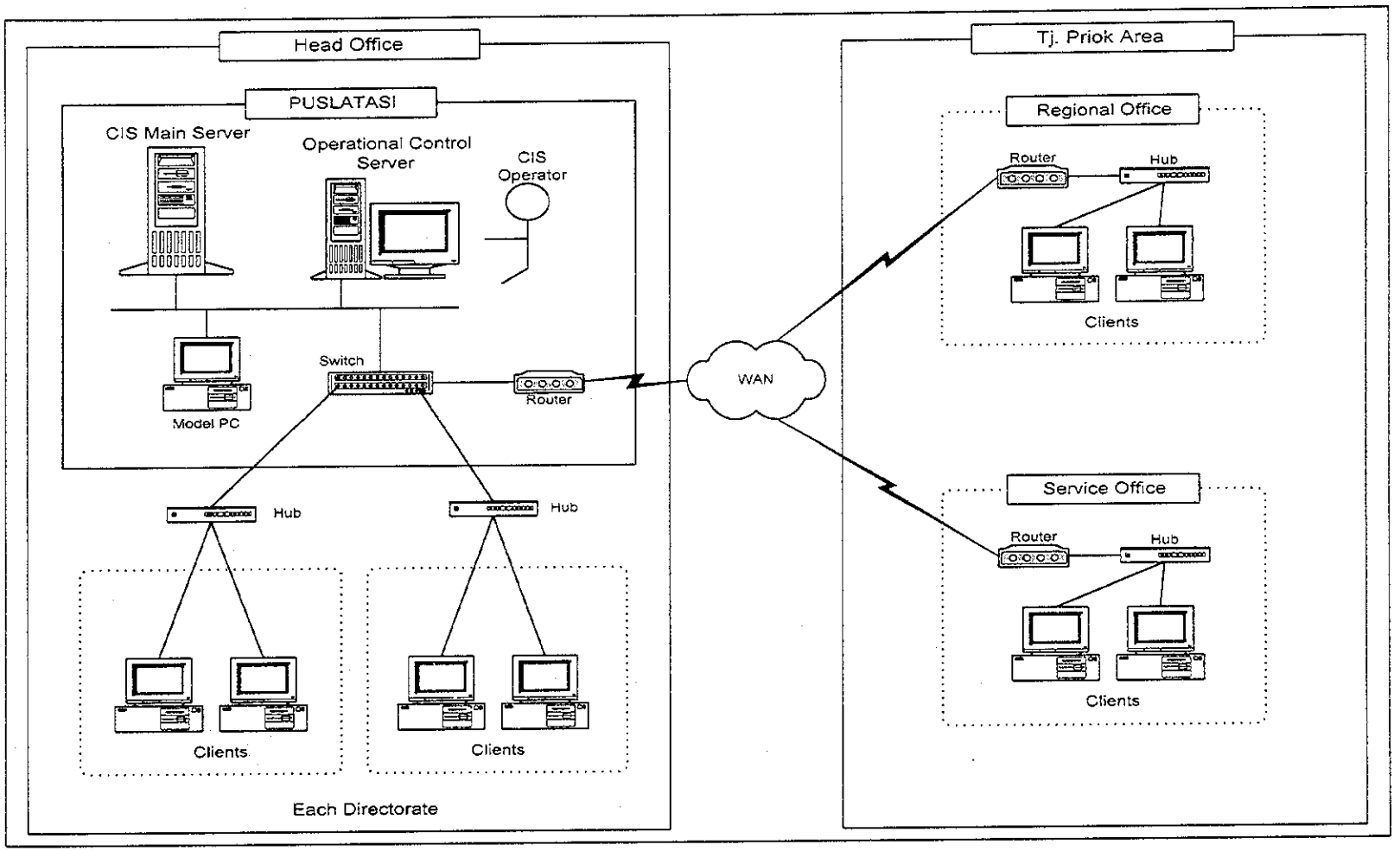

Figure 3.5.2-1: Overview of CIS Operation in the first stage

3.5.3 Operational organizations

This subsection includes proposals regarding operation of CIS from the aspects of organization in DJBC.

The topics discussed here are:

- Operating period of CIS

  General schedule of CIS service period.
- Work shifts in Head Office

  Work shifts in Head Office to support CIS operation.
- Operational rosters

  Organization of staffs and their roles in CIS.

In the following document, hours in timetables are presented as examples. Timetables are intended to show the jobs included in the operation and relation between jobs.

3.5.3.1 Operating period of CIS

Daily schedule of CIS service is divided into on-line and off-line operating period.

These are description of jobs to be performed during each period:

- On-line operating period (7:30 to 16:30)
  - End users perform their business processes through CIS clients in each office.
  - Operation staffs monitor CIS activity and performance.
  - Operation staffs solve hardware, network, and software problems.
- Off-line operating period (16:30 to 7:30)

  Off-line operating period is divided into batch operation time and spare time. For detailed information regarding batch operation time, refer to 3.9.2.3.

  Some of following tasks are automatically executed on the server. Operation staffs in PUSLATASI are in charge of monitoring them and perform manual tasks.
  - Batch operating period
    - Database backup processes
    - Gathering information from other systems (e.g. CFRS)
    - Update processes
    - Referential processes
    - Sending information to other systems

- Spare time
  - Maintenance tasks which require stopping CIS

CIS exchanges data with a number of CFRS installed in Service Offices. Some Service Offices operate 24 hours a day, while others do not. Schedule of the exchanges depends on the Service Office operation. At the first stage, Service Office of Tanjung Priok II operates 24 hours.

In Service Offices that do not operate 24 hours, there are no operators of CFRS during most of off-line operating period. Data exchange with such Service Offices should be done while operators are available.

Figure 3.5.3.1-1 shows the schedule of the exchanges between CIS and CFRS.

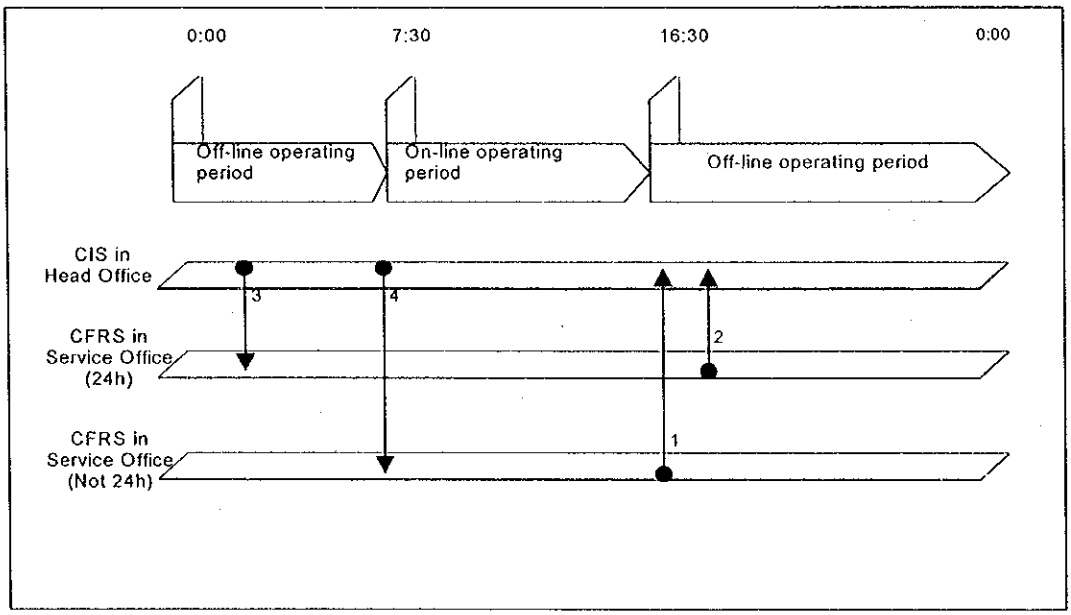

Figure 3.5.3.1-1: Data exchange schedule between CIS and CFRS

Followings are explanation of the figure. The numbers below correspond to those in the figure above:

1) Data of CFRS in the Service Offices, which are not operating 24 hours, are transferred to CIS during the end of on-line operating period and the time operators leave the office.
2) There are no such restrictions of transferring data of CFRS in the Service Offices, which are operating 24 hours. The data are exchanged before CIS starts updating processes.
3) After CIS creates data for sending, the data will be transferred to CFRS in the offices of 24 hours operation.

4) CIS will send the data to CFRS in the Service Offices of non-24 hours operation after the operation staff arrive at the office.

3.5.3.2 Work shifts in Head Office

The JICA Study Team presumes that CIS will be maintained 24 hours a day. Three work shifts are proposed to realize the continuous operation.

Figure 3.5.3.2-1 shows the relation between CIS operating period and the work shifts in Head Office.

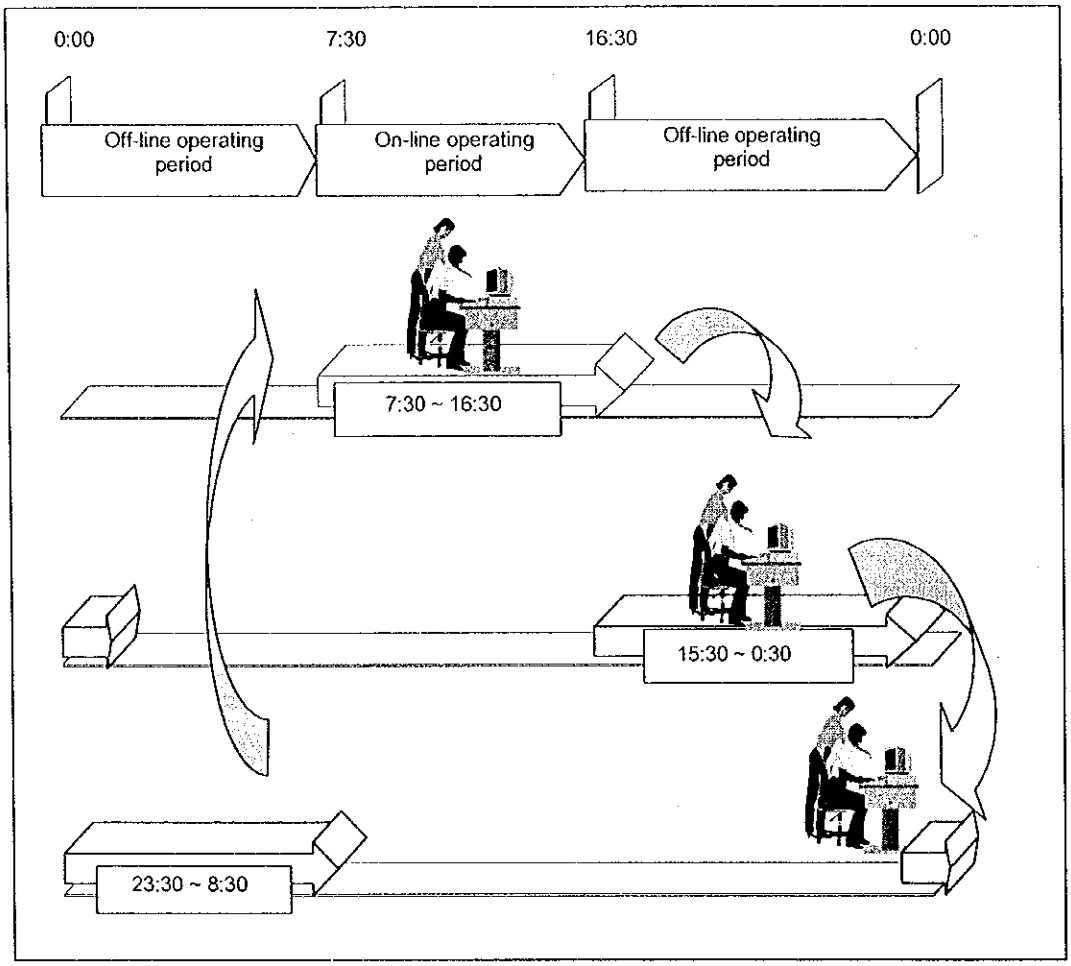

Figure 3.5.3.2-1: Relation between operating period and work shifts

These are conditions of each work shift:

- There are 3 work shifts for the CIS operations. Four groups work serially. From one shift to the next there is 1 hour of overlapping time.
- The Work shifts are :
  - From 7:30 to 16:30
  - From 15:30 to 0:30
  - From 23:30 to 8:30

Figure 3.5.3.2-2 describes a sample timetable of server operations for one-week period. In this example the JICA Study Team supposes 4 groups continuously work for 24 hours per-day and for 7 days per-week continuously. One group will consecutively work for 3 days and then one day off. According to this timetable, at least four groups work in shift to operate the CIS Main Server.

	One Week Period																													
Working Time	First day			Second day			Third day			Fourth day			Fifth day			Sixth day			Seventh day											
07:30~ 16:30	A	—		D	—		C	—		B	—		A	—		D	—		C	—										
15:30~ 00:30	—	B	—		A	—		D	—		C	—		B	—		A	—		D	—									
23:30~ 08:30	—		C	—		B	—		A	—		D	—		C	—		B	—		A									

Note: The four working groups are denoted as A, B, C and D.

Figure 3.5.3.2-2: Work shifts in one week

3.5.3.3 Operational rosters

The JICA Study Team proposes that each group at the Head Office consists of 4 (four) operators and only one operator at the Regional Office is needed. All of the operators work during DJBC working hours to maintain the CIS services.

Following document contains operational topic regarding Regional Servers that will be installed in second and later stage of CIS.

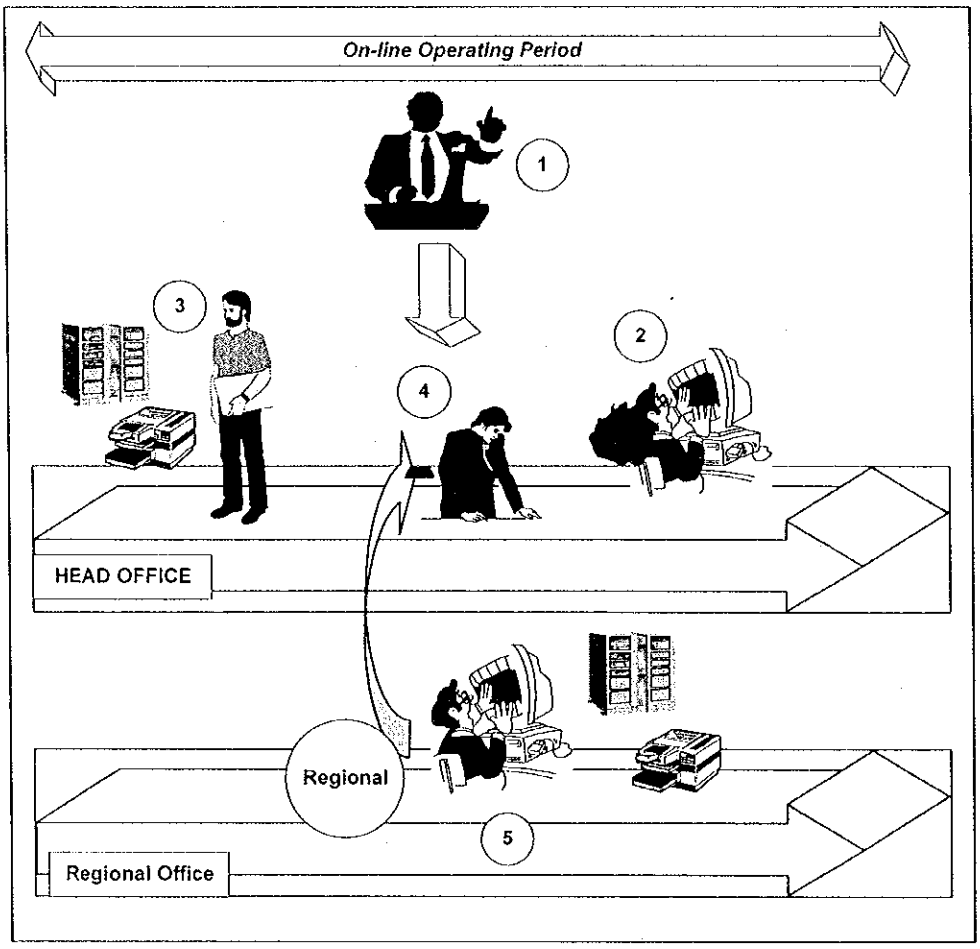

Figure 3.5.3.3-1: Operators during on-line operating period

During off-line operating period, no operator is on duty to handle CIS Regional Servers. Therefore, the CIS Main Server operators have to perform remote administration to handle the CIS Regional Servers.

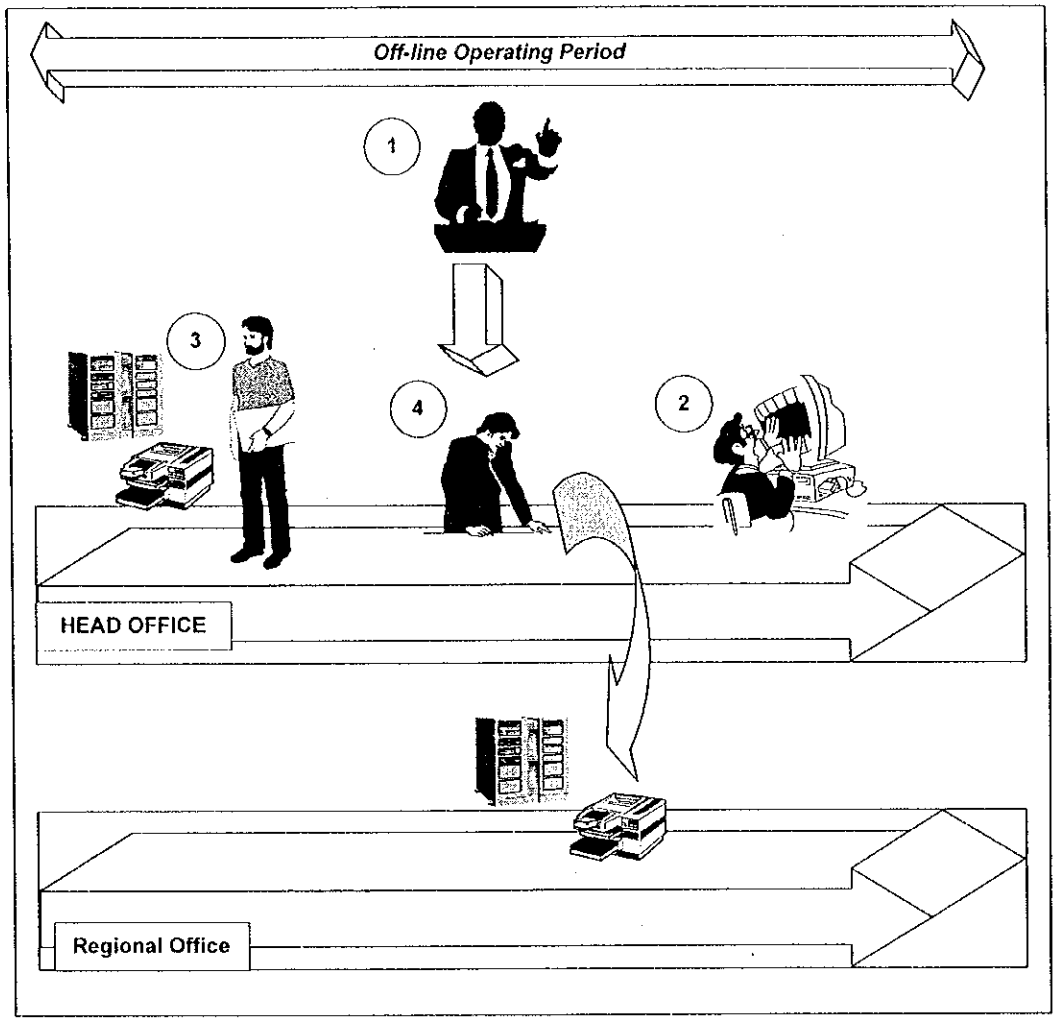

Figure 3.5.3.3-2: Operators during off-line operating period

Followings are proposal of organizational chart and descriptions of roles in the chart.

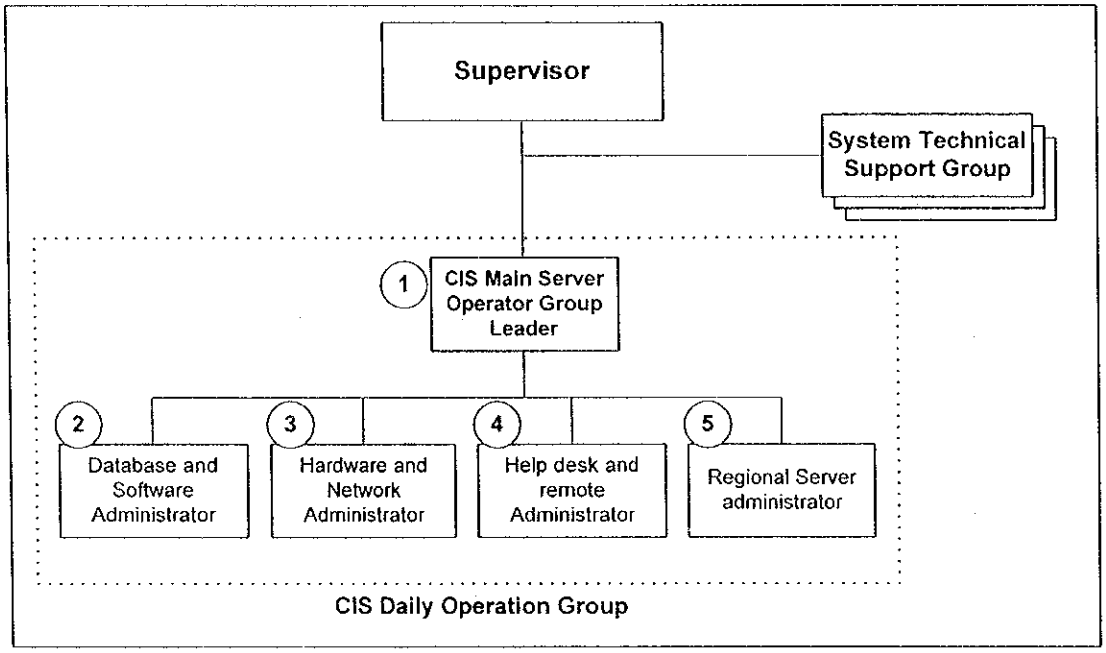

Figure 3.5.3.3-3: Operators relationship

Expertise and knowledge of operator could be divided into three levels such as:

- Advanced
- Intermediate
- Basic

Job description and skill for each operator are resumed on the table below.

Table 3.5.3.3-1: Job description and skills of operators (1/3)

Role	Job Description	Skill Requirement
Supervisor	In charge of managing all computer system operation.	• Advanced DJBC operation knowledge • Leadership
System Technical Support Group	In charge of supporting all computer system operation, high skill person is required.	• Advanced CIS operation knowledge • Advanced CIS application knowledge • Advanced Oracle database administration knowledge • Advanced Oracle system administration knowledge • Advanced hardware and network administration knowledge

Table 3.5.3.3-1: Job description and skills of operators (2/3)

Role	Job Description	Skill Requirement
CIS Main Server Operator Group Leader(1)(*)	• Establish standards of operation • Monitor CIS • Report to managements	• Advanced CIS operation knowledge • Intermediate CIS application knowledge • Intermediate Oracle database administration knowledge • Intermediate Oracle system administration knowledge • Intermediate hardware and network administration knowledge • Leadership
Database and Software Administrator (2)(*)	• Monitor database • Solve problems regarding database • Perform manual database management	• Intermediate CIS operation knowledge • Advanced CIS application knowledge • Advanced Oracle database administration knowledge • Basic Oracle system administration knowledge • Basic hardware and network administration knowledge
Hardware and Network Administrator(3)(*)	• Maintain Network Operation • Maintain Hardware Operation	• Intermediate CIS operation knowledge • Basic CIS application knowledge • Basic Oracle database administration knowledge • Advanced Oracle system administration knowledge • Advanced hardware and network administration knowledge
Help desk and remote Administrator(4)(*)	• Answer questions from operators in Regional Office • Record trouble incidents • Communicate with vendor • Record vendor support log	• Advanced CIS operation knowledge • Basic CIS application knowledge • Basic Oracle database administration knowledge • Basic Oracle system administration knowledge • Basic hardware and network administration knowledge

Table 3.5.3.3-1: Job description and skills of operators (3/3)

Rule	Job Description	Skill Requirement
Regional Server administrator(5)(*)	• Monitoring performance of Regional Server • Solving hardware, network and software problem • Inquire to help desk operator in Head Office	• Intermediate CIS operation knowledge • Intermediate CIS application knowledge • Intermediate Oracle database administration knowledge • Intermediate Oracle system administration knowledge • Intermediate hardware and network administration knowledge

Note: (*) These numbers are linked into the figure 3.5.3.3-1, 3.5.3.3-2, and 3.5.3.3-3.

3.5.4 Backup

Backup is to make copy of software information on disk system to semipermanent and removable media. When the information is lost from disk system, they are recovered from backup media.

Backup should be executed when the object is created or modified on the system. Following this principle, CIS backup can be divided into two categories:

- System backup

  Backup objects are software components to run CIS. This kind of objects is comparatively static until the configuration of system is changed.

- Data backup

  Backup objects are data used by daily business operations, which are stored in the CIS database. This kind of data is dynamically updated.

These two kinds of backup differ from the other in procedure. System backup should be performed after the installation of system or change of configuration. Data backup should be performed as one part of CIS daily jobs.

This subsection explains system backup of CIS. For data backup, refer to 1.8.7.2.

3.5.4.1 System backup of CIS

System backup policy of server is different from that of clients.

1) System backup of server

   Followings are the backup policy of CIS server.

   - Objects

     Backup objects are:

     - OS (execution files)
     - Definition files of environment
     - Definition files of users
     - Program products (ready-made products used in CIS)
     - User programs (custom-made CIS programs)

   - Media

     Magnetic tape media is used in backup. For reliability and performance of data transfer, the JICA Study Team proposes the use of DLT (refer to 3.8.2).

     Backup media should be kept following the procedure of DJBC security policy.

- Time to backup
  - When the system is installed for the first time.
  - After each change of configuration of server. Only changed component should be backed up.
- Recovery outline
  - If part of disk system is damaged, the information kept in damaged part should be selectively recovered from the backup media. Recovery must be performed after replacing the damaged part of disk system.
  - If the whole disk system is crashed, at first disk system itself should be re-constructed. Then all the backup data should be recovered from the backup media.

2) System backup of clients

Basically, the CIS clients will not be backed up since each client does not store specific information. When disk system of client is crashed, the failed disk system is replaced with new one and the client system is re-installed.

3.5.5 System monitoring

Activities of CIS, which are discussed in this subsection, are monitored in PUSLATASI. Operational control software supports integrated monitoring.

Figure 3.5.5-1 illustrates the system monitoring mechanism of CIS.

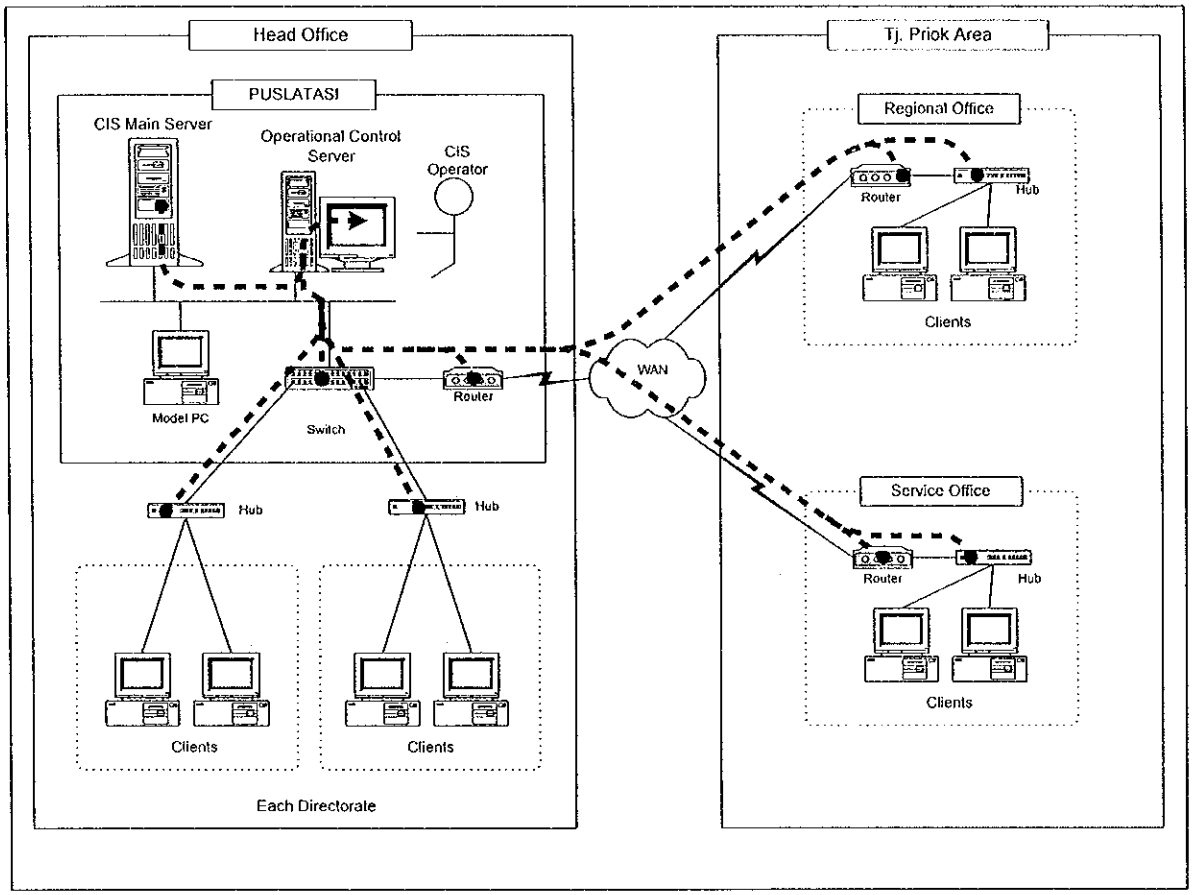

Figure 3.5.5-1: Mechanism of system monitoring

Operational control server gathers network configuration of the system automatically. Based on that information, activities of each component in CIS are graphically displayed on the screen of operational control server.

Major objects of system monitoring are the activities of the CIS Main Server and network.

Details of monitoring policy of CIS are explained in following sub-subsections.

When Regional Servers are installed in the second and later stage of CIS, they are monitored by operational control server just as the CIS Main Server.

3.5.5.1 Monitoring CIS Main Server

The operational control program is distributed to operational control server and the CIS Main Server. The server program is running on operational control server while the client program is running on the CIS Main Server. They are communicating each other through network. The client program running on the CIS Main Server enables monitoring activities on operational control server.

Operational control server monitors these kinds of activities of the CIS Main Server:

- Operation

  This means simply the CIS Main Server responds to the polling through network or not. If not, the CIS Main Server is not operating.

- Predefined failures

  Failures on the CIS Main Server are classified into several categories in accordance with their impact on the operation. Once the failures occur, they are called event. Serious events on the CIS Main Server are reported to operational control server. Threshold to filter events on CIS Main Server is configurable.

- Status of program products and user programs

  The program products and user programs are executed by job management function of operational control program, which is different from monitoring function.

  The monitoring and other management topics of these programs are discussed in 3.5.7.

- Status of database

  Performance and resource usage of the CIS database is monitored.

3.5.5.2 Monitoring CIS clients

Potentially, the operational control server can monitor activities of all the CIS clients. The monitored activity is whether each client responds to polling through the network or not. This monitoring is based on SNMP protocol.

However, some points require consideration regarding monitoring clients:

- Polling involves some network load. This may cause problems especially polling through WAN. There are WAN connection between operational control server and clients in Tj. Priok area.

- When one client does not respond to the polling, there are several causes. For example:
  1) The power of the client is turned off.
  2) The client is actually in trouble.

The monitoring policy of CIS clients should be reconsidered after investigation on actual machines used in development phase.

3.5.5.3 Monitoring network

Monitoring network involves two contents: monitoring network facilities themselves and monitoring traffics.

1) Monitoring network facilities

   This means monitoring of switch, router, hub, or other facilities support networking.

   Both simple monitoring, i.e. whether each facility is operating or not, and event monitoring are possible from operational control server. Events are predefined incidents on each facility.

   Network facilities are monitored by SNMP protocol.

2) Monitoring traffics

   The operational control server gathers statistical information of network traffic from each network facility. These informations are based on MIB-II.

   Traffic information is displayed on operational control server as graphical map.

   The operational control server stores traffic information; therefore both real-time monitoring and analysis of traffics following chronological order are possible.