

PN-ACC902

103816

United States Agency for International Development  
&  
Barents Group LLC

Technical Assistance to the  
Palestinian Monetary Authority

SEGIR GBTI  
Contract No PCE-I-800-98-00012

**FINAL REPORT on the Y2K PREPAREDNESS  
For the PALISTINIAN BANKING SECTOR**

USAID Contracting Technical Officer  
Nimi Wijesooriya

Barents Group LLC  
Project Manager  
Jay S Doeden

Prepared by  
Richard M Stitcher  
Stitcher & Associates, Inc

## **Executive Summary**

The Palestine Monetary Authority (PMA) has made significant progress in guiding and monitoring the Palestinian banking sector in its final preparations for the Year 2000 (Y2K) date transition at the end of December 1999. PMA management and senior staff have a good understanding of what is required and have moved steadily forward from the April 1999 visit by the prior USAID advisor to achieve a successful completion to this important project.

In this project the Barents Group LLC Y2K advisor received the ongoing assistance of the PMA's Senior IT Specialist who was responsible for guiding and implementing the details of the ongoing Y2K preparation program during 1999. A complete review of PMA's IT activities and an on-site visit to every bank in Palestine was accomplished.

The analysis of the interview notes and discussions with bank management leads this advisor to conclude and certify that overall readiness of the PMA and the Palestinian banking sector for Y2K are as complete as reasonably can be expected. There are still a relatively small number of exceptions to the total completion of several of the bank's individual Y2K planning processes. These items are fully detailed in the attached spreadsheet titled *Table 1-On-Site Visit Status Report-Summary Y2K Preparedness Comments For All Banks* (Table 1) that follows the narrative sections of this report. The exceptions generally do not threaten the IT Contingency or Business Continuity plans of these banks but are identified to more fully reduce, as much as practicable, any risks to the sector during the millennium period.

The banks as a group are generally well prepared for the millennium challenge. Senior managers at each bank have committed to timely resolution of every exception noted. Discussions with PMA Governor Beseiso gave strong assurances that close follow-up by PMA staff will assure elimination of all exceptions prior to December 31, 1999. At a general level across the sector the advisor believes that both the PMA and the Palestinian banks can fully address any disruptions to processing or business operations that may occur over this period in a timely and accurate fashion. If there are disruptions in the country's infrastructure (electrical supply, telephone service, telecommunications networks, etc.) these organizations are also well prepared to both cope with and overcome such hindrances to banking operations. The high level of preparedness is directly tied to the PMA's active guidance to the banking sector over this past nine months. As a final safeguard and protection for banking operations the PMA has required every bank to develop and test a fallback to manual processing, if necessary. Such depth in planning has provided a high level of protection to the Palestinian banking sector and the customers they serve.

In addition to the specific exceptions noted for several of the banks in Table 1 there are also several appendices to this report, which provide guidance to the PMA in initiating a public awareness program (newspaper advertisements) over these final two weeks of the millennium and for the establishment of a PMA Y2K Command Center. These areas are more fully detailed later in this report.

## Scope of the Project

According to the USAID Terms of Reference, the objective of this review were to

- Review and verify the critical system's lists within the banks and the Palestine security Exchange (HW/SW, applications and embedded systems) to ensure correctness of these lists and update them as needed
- Assess all times on the critical system's lists to ensure that they are Y2K compliant by conducting a Y2K simulation testing without any manual intervention,
- Review all test results and Y2K documentation
- Issue an Y2K statement of compliance for each bank and Palestine Securities Exchange, which should be approved by the PNTC
- Review and evaluate existing contingency plans for each bank and Palestine Securities Exchange and update the plan as required
- Supervise and monitor a sector-wide drill to make sure that contingency plans and Y2K emergency systems would work when needed This is important in order to make sure that the banking sector will be prepared for December 31, 1999

This review substantially complied with and was completed in accordance with the original terms of reference USAID approved exceptions are as follow

- Verbal instructions were received from the USAID CTR Nimi Wijesooriya on December 16, 1999 that the Y2K advisor was explicitly instructed not to review the Palestine Securities Exchange (PSE) for Y2K readiness although it had been scheduled under the original terms of reference This decision was made after USAID management realized that the PSE was a privately owned organization and that it was not legally under the authority of the Palestinian National Authority or the PMA
- The second exception related to the fact that there was insufficient time for the advisor to conduct a Y2K simulation testing without any manual intervention or to direct and review the results of a simultaneous three day manual processing exercise by the 21 banks in this sector of the economy

Notwithstanding the short-term duration of this review (as compared to the original schedule of two advisors for 30 and 52 days, respectively), the time necessary to meet with bank management and to conduct the interviews, and the lack of formal plans and documentation maintained, the advisor substantially met each of the objectives outlined above

## Background

A Barents Group IT expert and technical advisor completed a three-week Y2K review of the 21 banks licensed and operating in the West Bank and Gaza The purpose of this final Y2K preparedness review was to evaluate the readiness of each bank to handle and appropriately respond to the issues and potential problems associated with the Y2K date transition event

The advisor met employees of the banks at the senior and middle management levels. He also met with PMA's IT management and staff and with senior operations management. The advisor held two briefings during this visit with PMA Governor Fouad Beseiso.

In addition to the on-site bank review, the advisor conducted a review of the PMA internal readiness and preparedness for the Y2K. This report includes the advisor's findings and conclusions relative to the PMA and banks reviewed. It also addresses recommendations for a proposed PMA public awareness program and provides practical guidance for PMA in the setting up of an Y2K Command Center.

## **Findings and Conclusions**

### **▪ General Assessment of the PMA's Y2K Initiatives**

#### **Conclusion**

Although the PMA started later than many other banking regulatory agencies it has made substantial progress during 1999 in assuring that the banking sector of Palestine will be well prepared to successfully maintain operations over the millennium date change period.

Throughout the West Bank and Gaza, banks are for all intents and purposes positioned to cope with most foreseeable internal or external processing disruptions that may occur. Much of the progress in this area can be attributed to

- the establishment of an Y2K Committee of bankers that is comprised of banking and IT professionals from all the banks and led by the PMA. This committee has met monthly or more frequently since the April 1999 review. The committee has provided guidance, direction and structure to all of the Palestinian banks. It has provided the PMA with an extremely effective two-way communications channel to every bank under its jurisdiction and allowed them to address collaboratively common problems and share critical information to assist in their preparations.
- the requirement that every bank would submit their Y2K Project plans to the PMA by June 30, 1999. Each bank was also required to submit its Y2K Contingency plans to the PMA by September 30, 1999. These plans outlined each bank's Y2K program as well as forcing the development of operational contingency plans which covered all IT activities in the bank and also provided for the resumption of normal banking/business activities in the event of an emergency.
- the PMA established and monitored each bank's progress in adhering to Y2K specific guidelines and timeframes for planning, fixing, testing and implementation of remediation.
- the PMA's dedication of a full-time employee from the IT area to oversee the program. This IT Senior Specialist has done an excellent job of managing the flow of documents from the banks and also in their review and in initiating feedback when appropriate in order to ensure banking compliance with PMA's directives.
- the PMA needed to develop an awareness program to inform the public of the Year 2000 challenges and the work the PMA and banks are doing to meet these challenges. This was

the one area of activity that was recommended at the April visit where the PMA was unable to accomplish the task

- the PMA initiated and has completed its own internal Y2K remediation program to ensure the agency's compliance with Y2K requirements

### **Finding**

Meetings were conducted with Governor Beseiso and staffs from the IT and senior operations management in the West Bank and Gaza offices. The Y2K preparation steps taken to date by the PMA were reviewed and discussed. All instructions to the banks and the results of workshops held with the banks were reviewed and evaluated. The on-going minutes of the PMA's Y2K technical committee were reviewed and discussed. Meetings were held with representatives of the Palestinian National Authority's Technical Y2K Committee. At the previous review the Governor appointed two staff members (a senior manager and an IT Senior Specialist) to coordinate the PMA efforts.

### **▪ Banking Sector's Y2K Preparedness Status**

### **Conclusion**

All banks have developed workable contingency plans for their IT operations and business activities. As noted in the attached spreadsheets labeled Table 1 through Table 4 some banks still must make minor improvements to their individual plans in order to consider them complete. The exceptions which are in the process of correction covered:

- Finalization of the manual processing fallback position by performing a complete test of this approach across all areas of the bank
- Contact being made with significant borrowers and depositors of the bank to determine that they too (if reliant upon IT activities in their business activities) were also properly prepared to operate efficiently through the millennium date change
- In the area of liquidity planning some bankers had not developed a Y2K oriented liquidity plan which would prepare them for unusually higher outflows of currency over this period of time
- The need for a temporary increase in the bank's insurance coverage over that period where excess currency was being maintained in order to ensure an adequate level of liquidity

Overall the banking sector is well positioned for the millennium date change. This advisor received strong management commitments in every institution that would ensure all exceptions were to be corrected prior to yearend. Additionally, the PMA Governor committed all of the needed resources to track every exception in the bank to completion.

### **Finding**

Every bank in Palestine was visited and an interview was held with senior management and the most senior IT manager. Information was developed from these visits across several areas of the bank's preparations for the Y2K event. See appendices A, B, and C which address the schedule of bank visits, the officers of the bank who were met, and a sample interview/data input form is provided to show the area of questioning which was covered at

5

each interview. In general, banks have a good understanding of the Year 2000 issues and have devised strategies to handle the problems and find solutions. At present every bank in Palestine has completed the remediation necessary to ensure an efficient transition to the next millennium as regards their IT operations and general business operational issues. The banks have swapped out or fixed all IT hardware and corrected or replaced embedded date dependent systems. All operating software, application software and supporting networking structures (LAN and WAN) have been fixed. Testing has been completed and reviewed.

The major shortfall observed during the on-site visits as regards the banking sectors preparation for Y2K was seen in the case that several banks seem to still be considering this to be primarily an IT issue (see table 1).

- **PMA's Preparedness for Y2K**

#### **Conclusion**

The PMA is well prepared to address processing across its organization in the new millennium. The PMA's operational and IT processing activities are basic in nature and therefore are much less susceptible to the Millennium Bug. Most processing currently occurs on PC's and/or small servers that are currently using Microsoft Access databases and Excel spreadsheets as the basis for their processing. This made all software upgrades relatively easy through the use of downloaded Service Pack Update Releases from Microsoft's home page on-line.

#### **Finding**

The PMA's staff has fully prepared the operations on the organization to ensure proper processing for the Y2K transition. A full review of documentation reflected that ALL PMA IT hardware and embedded logic chip oriented technology had been remediated. PMA contracted with an outside firm to come on premises and validate that all hardware and operating systems were Y2K compliant. As an abundance of caution they continue to run Y2K Diagnostic Software on resident PCs to ensure continuing compliance. They also upgraded all operating system and application system software. In the Clearing area only partial automation is in place and there is still a heavy reliance on manual processing to accomplish daily operations. PMA has also developed a full set of current procedures that allow a full fallback to manual processing across all activities in the organization.

### **PMA's Public Awareness Program**

#### **Conclusion**

Recommendations were made to PMA management in three areas of public awareness for Y2K. These draft newspaper announcements are located in Appendices D through H and address several topics. Since there has been no activity in this area previously it is recommended that the first announcement cover the degree of preparations the banking sector have made as regards Y2K (appendix D) and that in all cases banks have developed contingency and business resumption plans that allow a complete recovery in the event there are any Y2K related degradations should occur. The PMA should inform the public that the banks are also prepared for disruption that may occur in the country's infrastructure (power, telephone, telecommunications, etc.) Confirming and assuring that the banking sector is well prepared for Y2K should be the first step. Follow-on to this there should be an announcement to the public indicating some common questions and answers that may come

up to again provide basic information to relieve concern or potential stress among the banking Palestinian public (appendix E) The last recommended announcement in this area is related to the potential that criminals may try to take advantage of this potentially unsettled period of time and perpetrate frauds on banking customers (appendix F) This announcement should address some common approaches used by criminals and give short and concise precautions that the public should take

In another area this advisor provided a draft procedure addressing how individuals can better protect their PC's and software against viruses (appendix G) This document should be issued to the staff across the PMA in order to provide a common and consistent level of direction to all employees in this area of IT The six common steps to avoid and control computer viruses should provide a level of protection against future attacks on PMA databases and hardware The last draft announcement that is being recommended is more generic in nature and was recommended to the representatives of the Palestinian National Authority's Y2K Technical Committee (see appendix J) who were present at the closeout meeting held with PMA's Governor and his staff This draft announcement provides a general level of guidance to the public as to areas where they might wish to make specific Y2K related preparations in the event there is infrastructure disruption in Palestine (appendix H)

The Palestinian public does not need to see a barrage of Y2K related announcements over the final 2 weeks of the century A few well placed advertisements should help PMA inform but not alarm the public as to the level of preparation that has been developed across Palestine's banking sector

### **Finding**

PMA management had not developed program of advertising (newspaper is recommended) to inform the Palestinian public that the banking sector within the country was Y2K compliance The PMA's senior management is well aware of the need for such an awareness program and requested this advisor's assistance in developing one Several draft newspaper announcements were presented to PMA management for their consideration during the later part of the assignment They are actively considering using these as the basis for a newspaper campaign to inform the public about Y2K readiness in the banking sector of Palestine

- **Banking Holiday on January 2, 2000**

### **Conclusion**

At the Banker's Y2K Workshop, held on the evening of December 15, 1999, the topic of a bank holiday for the Sunday after New Year's Day was raised by several bankers who were at the meeting The Governor solicited discussion on this topic and after consultation with the representative from the PNA's Technical Y2K Committee a decision was announced that Sunday January 2, 2000 would be a banking holiday for all Palestinian banks This announcement was incorporated into the draft newspaper advertisement (appendix D) covering the safety and the preparations that had been made regarding Y2K by the banks of Palestine

### **Finding**

During the course of several on-site interviews senior bank managers and their IT officers indicated concern that the PMA had not decided to declare January 2, 2000 as a banking

holiday in order to give the banks some additional time to recheck and test their preparations for Y2K

- **Establishing a Y2K Command Center**

### **Conclusion**

The Bank for International Settlement in Basel, Switzerland has addressed the problem of Y2K related Bank-Supervisor communications and also the cross-border issue of Banking Supervisor to Banking Supervisor communication in areas where supervisory authority may have a common interest. Attached to this report are two documents labeled appendices K and L. Appendix K is titled "Gathering Y2K Information From Financial Institutions Recommendations for Supervisors". This document provides very clear direction to the supervisor as to how to set up an emergency command center capable of tracking any Y2K related disruptions in the individual banks or across the banking sector as a whole. It is critical that PMA be in close contact with its banks from December 31, 1999 when the traditional yearend processing will occur through and including January 3, 2000 which will be the first business day in the new year and the new millennium. The banks will be staffed across this weekend doing a last minute series of Y2K-related tests to ensure total compliance with Y2K. It is important that the PMA also be staffed across this 5-day period. It is recommended that, at a minimum one banking supervisor and one IT Specialist is present on a 24 hour a day basis across this extended weekend. If PMA follows the guidance provided by the BIS Circular they should be adequately prepared to run their **Y2K Command/Emergency Center**.

Appendix L is entitled "Y2K Cross-Border Communications Between Supervisors During the Millennium Period" and can be used to provide PMA both direction and guidance in establishing appropriate channels of communication from the PMA to other Banking Supervisory Departments, to the PNA's Y2K Technical Committee and to any other appropriate recipient. Many of the banks in Palestine are affiliated with and have their head offices in Jordan. Two banks in the Palestinian system are affiliated with banks in Egypt. All of the banks in Palestine have access to Israel's Central Bank. It is important that PMA's management establish clear, formal and reliable lines of communication with these other bank supervisors as well as with the PNA's Y2K Technical Committee. Governor Beseiso assured the advisor that the **Y2K Command/Emergency Center** would be set up and fully tested prior to year end to ensure reliable communications and status reporting both to and from the Palestinian banks as well as to other Cross-Border entities as necessary.

### **Finding**

Senior management of PMA had not had time to address the establishment of an **Y2K Command/Emergency Center**. It was strongly recommended that PMA needed a reliable channel of communications through which they could stay in bilateral contact with all of the banks in the sector over the period of the extended Millennium weekend. It is critical that PMA management has a structured way to communicate with the banks and that the bankers have a structured way to communicate with PMA in the event of Y2K related disruptions. By having such a center PMA will be able to ensure that they maintain effective supervisory authority with their banks. Correspondingly the bankers will have a channel to report internal or external Y2K disruptions to their regulator in the event that they cannot deliver normal and traditional banking services to their customers as required.

## **Appendices - Tables**

- Table 1 - On-Site Visit Status Report - Summary Y2K Preparedness Comments For All Banks
- Table 2 - On-Site Visit Status Report - Contingency/Business Continuity Planning
- Table 3 - On-Site Visit Status Report - Customer Involvement, Training and Liquidity Planning
- Table 4 - On-Site Visit Status Report - Progress on Items Referenced in April 99 Y2K Report

## **Appendices – Exhibits**

- A Appointment Schedule Listing Date, Time, and Location of Each bank Visit
- B Listing of All bank Officers Met During On-Site Visits
- C Bank Interview/data Input Form
- D Recommended Draft Newspaper Announcement Addressing Ability of Palestinian Banks to Do Business Through Millennium date Change
- E Recommended Draft Newspaper Announcement Listing Several Common Y2K Related Questions and Answers
- F Recommended Draft Newspaper Announcement Addressing a Y2K Fraud Warnings for the Citizens of Palestine
- G Recommended Draft Procedure for PMA Staff Covering Common Sense Rules to Protect Your PC from Viruses
- H Recommended Draft Newspaper announcement for PNA Identifying Practical Hints on Y2K for the General Public
- I Transcription (English) of the Press Release Made by PMA Detailing the Substance of the Meeting/Workshop Held on 12/15/99 By Senior PMA management, this Advisor and Senior managers from All Banks
- J Listing of the PNA Members of the National Authority Technical Y2K Committee
- K BIS (Basel) Issuance Covering “Gathering Y2K Information From Financial Institutions recommendations for Supervisors”
- L BIS (Basel) Issuance Covering “Y2K Cross-Border Communications Between Supervisors During the Millennium Period”

**Part 1 - On-Site Visit Status Report - Summary Y2K Preparedness Comments For All Banks**

<b>Bank/Branch</b>	<b>Is Followup Needed</b>	<b>Areas of Followup Required (if any)</b>	<b>Final Y2K Preparedness Rating</b>	<b>Final Summary Comments</b>
	<b>Yes or No</b>			
<b>HSBC Bank</b>	<b>NO</b>	<b>None Required</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>ANZ Grndlays Bank</b>	<b>NO</b>	<b>None Required</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Al-Quds Bank Investment &amp; Development</b>	<b>YES</b>	<b>Gen Mgr promised fax to PMA 12/26 with full update 1 Manual test performed? What were results? visit large credit &amp; deposit customers Are Customers Y2K ready? Will they get additional insurance for extra currency?</b>	<b>Fair to Good - Should be OK if promises kept and manual Test results were OK</b>	<b>Good IT Planning, Good Business Contingency Plan Good Liquidity Planning Should be OK if Manual test was good</b>
<b>Union Bank for Savings &amp; Investments</b>	<b>YES</b>	<b>1 Did they visit all large credit/deposit customers by 12/24? Are they Y2K prepared?</b>	<b>Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Cairo Amman Bank</b>	<b>NO</b>	<b>None Required</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>

TABLE 1  
Pg 1 of 4

**Part 1 - On-Site Visit Status Report - Summary Y2K Preparedness Comments For All Banks**

<b>Arab Land Bank</b>	<b>NO</b>	<b>None Required</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Palestine International Bank</b>	<b>YES</b>	<b>1 Did they do Integrated test of IT Systems as promised 2 Were Manual training plan/test developed/performed? 3 Was extra currency insurance coverage acquired if needed?</b>	<b>Good if Integrated IT test and Manual test results showed no problems</b>	<b>Good IT Planning but need to do integrated test, Good Business Contingency Plan and Manual Fallback if test was OK Good Liquidity Planning</b>
<b>Palestine Investment Bank</b>	<b>YES</b>	<b>1 Was an integrated manual test performed no later than 12/28 as promised by management? What were results?</b>	<b>Good if integrated manual test worked OK</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback if test was OK Good Liquidity Planning</b>
<b>Arab Bank</b>	<b>YES</b>	<b>1 Did they visit large credit/deposit customers? Are they Y2K prepared?</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Arab Palestine Investment Bank</b>	<b>YES</b>	<b>1 Was Manual test performed for 3 days from 12/18-20 as promised by management? What were results?</b>	<b>Very Good if Manual test results were OK</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>

**Part 1 - On-Site Visit Status Report - Summary Y2K Preparedness Comments For All Banks**

<b>Commercial Bank of Palestine</b>	<b>YES</b>	<b>1 Did they visit large credit/deposit customers? Are they Y2K prepared? 2 Was extra currency insurance coverage acquired if needed?</b>	<b>Good to Very Good if comments to left were resolved</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Bank of Jordan</b>	<b>YES</b>	<b>1 Did they visit large credit/deposit customers directly? Are they Y2K prepared? 2 Was extra currency insurance coverage acquired if needed? Did they check with Amman head office?</b>	<b>Good to Very Good if comments to left were resolved</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Jordan National Bank</b>	<b>YES</b>	<b>1 Did they visit large credit/deposit customers (25)? Are they Y2K prepared?</b>	<b>Very good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>AL-Aqsa Islamic Bank</b>	<b>NO</b>	<b>None Required</b>	<b>Very Good</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>
<b>Arab Islamic Bank</b>	<b>YES</b>	<b>1 Did they visit large credit/deposit customers directly? Are they Y2K prepared? 2 Was extra currency insurance coverage acquired if needed? 3 Did they make currency arrangements with correspondents as promised?</b>	<b>Good to Very Good If insurance and currency issues resolved</b>	<b>Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning</b>

12

**Part 1 - On-Site Visit Status Report - Summary Y2K Preparedness Comments For All Banks**

Jordan Gulf Bank	YES	1 Was extra currency insurance coverage acquired if needed? Did they check with Amman head office?	Very Good	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning
Housing Bank	NO	None Required	Very Good	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning
Jordan Kuwait Bank	YES	1 Was extra currency insurance coverage acquired if needed? Did they check with Amman head office? Liquidity Plan developed? correspondents supply currency needs? 2 Was Y2K 3 Will	Good if areas mentioned were corrected	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning
Bank of Palestine, Ltd	NO	None Required	Very Good	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning
Palestine Islamic Bank	YES	1 Did they visit large credit/deposit customers directly (50)? Are they Y2K prepared? Not as significant as in other banks due to strong general customer awareness program performed since June 1999 Promised to visit before year end	Very Good where the visiting of prime customers will just make it a little better overall	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning
The Principal Bank/Egypt	YES	1 Did they visit large credit/deposit customers directly (only 6 or 7 customers involved who may have IT dependent businesses as most customers are farmers)? Are they Y2K prepared?	Good to Very Good overall	Good IT Planning, Good Business Contingency Plan and Manual Fallback Good Liquidity Planning

## Part 2 On-Site Visit Status Report - Contingency/Business Continuity Planning

Bank/Branch	Y2K Contingency Plan Current	Date Plan Tested	Date Plan Modified (if needed)	Date Plan Retested (if needed)	Manual Processing Fallback	Date Tested	Copy of Customer Data Base Maintained (Both Hardcopy and on Disk Remote)
HSBC Bank	Current IT Plan	Oct 99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office
ANZ Grindlays Bank	Current IT Plan	Sep-99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Al Quds Investment & Development	Current IT Plan	Oct 99	na	na	No Test	Will be Done by 12/24	Customer Statements held at home closest office
Union Bank for Savings & Investments	Current IT Plan	Jun 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Cairo Amman Bank	Current IT Plan	Oct 99	na	na	Tested and Adequate	Sep 99	Customer Statements held at home closest office
Arab Land Bank	Current IT Plan	Sep 99	na	na	Tested and Adequate	Oct 99	Customer Statements held at home closest office
Palestine International Bank	Current IT Plan	Will be done by 1/17	na	na	No Test	Will be done by 12/20	Customer Statements held at home closest office
Palestine Investment Bank	Current IT Plan	Oct 99	na	na	No Test	Will be Done by 12/17	Customer Statements held at home closest office
Arab Bank	Current IT Plan	Jun 99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Arab Palestine Investment Bank	Current IT Plan	Oct 99	na	na	Not Test	Will be done between 12/18-20	Customer Statements held at home closest office
Commercial Bank of Palestine	Current IT Plan	Sep 99	Nov 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Bank of Jordan	Current IT Plan	Oct 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Jordan National Bank	Current IT Plan	Oct 99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Al Aqsa Islamic Bank	Current IT Plan	Oct 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Arab Islamic Bank	Current IT Plan	Oct 99	Nov 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Jordan Gulf Bank	Current IT Plan	Nov 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Housing Bank	Current IT Plan	Oct 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Jordan Kuwait Bank	Current IT Plan	Oct 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Bank of Palestine Ltd	Current IT Plan	Jun 99	Oct 99	Nov 99	Tested and Adequate	Nov 99	Customer Statements held at home closest office
Palestine Islamic Bank	Current IT Plan	Nov 99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office
The Principal Bank/Egypt	Current IT Plan	Jul 99	na	na	Tested and Adequate	Nov 99	Customer Statements held at home closest office

Table 2  
Page 1 of 1

14

### Part 3 - On-Site Visit Status Report - Customer Involvement, Training and Liquidity Planning

Bank/Branch	Bank completion of a Self Assessment Survey for PMA	Use of Customer Questionnaires By Banks	Use of Customer Credit Assessments By Banks	Adequacy of Customer Involvement Program	Adequate Insurance and Physical Security	Adequate Y2K Liquidity Plan
HSBC Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
ANZ Grindlays Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
Al-Quds Investment & Development	Yes Completed 7 99	Yes	Not done	Fair Will correct	Will Check Insurance	None To be done
Union Bank for Savings & Investments	Yes Completed 7 99	Yes	Not done	Fair Will correct	Yes on both	Good Plan 10%
Cairo Amman Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
Arab Land Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
Palestine International Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 7% 8%
Palestine Investment Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
Bank of Jordan	Yes Completed 7 99	Yes	Not done	Fair Will correct	Will Check Insurance	Good Plan 8% 10%
Commercial Bank of Palestine	Yes Completed 7 99	Yes	Not done	Fair Will correct	Will Check Insurance	Good Plan 8%
Jordan National Bank	Yes Completed 7 99	Yes	Not done	Fair Will correct	Yes on both	Good Plan 10%
Arab Bank	Yes Completed 7 99	Yes	Not done	Fair Will correct	Yes on both	Good Plan 10%
Arab Palestine Investment Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 10%
AL Aqsa Islamic Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 9% 10%
Arab Islamic Bank	Yes Completed 7 99	Yes	Not done	Fair Will correct	Will Check Insurance	Good Plan 10%
Jordan Gulf Bank	Yes Completed 7 99	Yes	Yes	Good	Will Check Insurance	Good Plan 10%
Housing Bank	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 8% 10%
Jordan Kuwait Bank	Yes Completed 7 99	Yes	Yes	Will Check insurance	Will Check Insurance	New Goal 10%
Bank of Palestine Ltd	Yes Completed 7 99	Yes	Yes	Good	Yes on both	Good Plan 7% 10%
Palestine Islamic Bank	Yes Completed 7 99	Yes	Not done	Fair Will correct	Yes on both	Good Plan 10%
The Principal Bank/Egypt	Yes Completed 7 99	Yes	Not done	Fair Will correct	Yes on both	Good Plan 10%

13  
 Page 1 of 1  
 1304-1

## Part 4 - On-Site Visit Status Report - Progress on Items Referenced in April 99 Y2K Report

Bank/Branch	Y2k Preparation Status Review	Written Plan	Awareness		Assessment (Written Inventory)	Validation (Testing)	Renovation (Repair)	Implement	Summary Comments/Evaluation after December 1999 Bank Visit
			Employees	Customers					
<b>HSBC Bank</b>	April 99 Status	HO	Yes	Yes	Yes	Yes	Not Required	Yes	Recently opened Systems tested prior to opening Banking system is Y2K compliant Plans and renovation work done on a Group level in Dubai (Very Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>ANZ Grindlays Bank</b>	April 99 Status	HO	Yes	Yes	Yes	Limited	Not Required	Yes	Recently opened Systems tested prior to opening No integrated test Maintains good documentation (Very Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Jerusalem Investment &amp; Development</b>	April 99 Status	No	No	No	Yes	Limited	No	No	Hardware is being replaced Software provided by an outside vendor and is being upgrading (Fair)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Union Bank for Savings &amp; Investments</b>	April 99 Status	HO	Limited	No	No	Very Limited	No	No	Banking system written in COBOL and being upgraded HO coordination is limited Branch resources appear to be limited (Needs improvement)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Cairo Amman Bank</b>	April 99 Status	HO	No	No	Yes	No	No	No	Replacing and upgrading in June Software provided by an outside vendor (Needs improvement)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Arab Land Bank</b>	April 99 Status	HO	No	No	Yes	No	No	No	Replacing and upgrading in June Software provided by an outside vendor (Needs improvement)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

## Part 4 - On-Site Visit Status Report - Progress on Items Referenced in April 99 Y2K Report

<b>Palestine International Bank</b>	April 99 Status	In May	No	No	Yes	Limited	No	No	In house committee consist of IT and administration and often communicates through e-mail with IT and branches (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Palestine Investment Bank</b>	April 99 Status	No	No	No	Yes	Limited	No	No	Unit test has been completed but no documentation Software is being upgrading (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Bank of Jordan</b>	April 99 Status	HO	Yes	Yes	Yes	Limited	No	No	Software being upgraded Plans are driven by HO (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Commercial Bank of Palestine</b>	April 99 Status	No	No	Limited	Yes	Limited	No	No	Plans to upgrade to software and hardware Testing has involved user groups (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Jordan National Bank</b>	April 99 Status	HO	Yes	Limited	Yes	Limited	No	No	Regional committee consisting of HO branch and IT staff Software provided by outside vendor is being upgraded (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Arab Bank</b>	April 99 Status	HO	Yes	Yes	Yes	Yes	Yes	Not completed	Testing has been mostly completed In house programs are Y2K compliant outside programs are being upgrading HO assurance team to visit in May HO committee consists of senior managers from branches HO has developed contingent plans (Very good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant
<b>Arab Palestine Investment Bank</b>	April 99 Status	HO	No	No	No	No	No	No	Small bank with mostly wholesale operations Few customers and products Owned 50% by Arab Bank Works with and has technical agreement with Arab Bank (Good)
	December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

## Part 4 - On-Site Visit Status Report - Progress on Items Referenced in April 99 Y2K Report

**AL-Aqsa Islamic Bank**

April 99 Status	Yes	No	No	Yes	Limited	Not Required	Yes	Recently opened with few customers Systems tested prior to opening No integrated test (Very Good)
December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

**Arab Islamic Bank**

April 99 Status	HO	Limited	Limited	Yes	Limited	No	No	In house committee consist of IT staff Software provided by an outside vendor and in the process of being upgrading (Good)
December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

**Jordan Gulf Bank**

April 99 Status	HO	No	No	Yes	No	No	No	PCs replaced Software provided by an outside vendor and is being upgrading (Good)
December 99 Status	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant						

**Housing Bank**

April 99 Status	HO	No	Limited	Yes	Limited	No	No	PCs replaced Software provided by an outside vendor and is being upgrading (Good)
December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

**Jordan Kuwait Bank**

April 99 Status	HO	No	Limited	No	No	No	No	Upgrading of hardware in progress HO committee will visit in May (Good)
December-99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

**Bank of Palestine, Ltd**

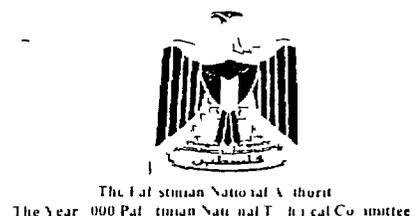
April 99 Status	No	Yes	No	No	No	No	No	Software provided by outside vendor Plans to upgrade to software and hardware Needs to formalize in house committee (Fair)
December-99 Status	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant						

**Palestine Islamic Bank**

April 99 Status	No	Yes	No	No	Limited	No	No	Plans to upgrade to software and hardware Testing has involved user groups (Fair)
December 99 Status	YES	YES	YES	YES	YES	YES	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant

**The Principal Bank**

April 99 Status	No	Operations are mostly manual HO committee plans to visit the branch in May (Needs Improvement)						
December 99 Status	YES	All Hardware and software Y2K Compliant and Certified as required All Non IT Compliant						



## Palestine Monetary Authority (PMA) Bank Y2K Review Project

Bank/Branch	Dates of Dec-1999 On-Site Bank Visits
HSBC Bank Middle East	Ramallah 12-07-99 10:00-12:00
ANZ Grindlays Bank	Ramallah 12-07-99 12:30-2:30
Al-Quds Bank for Development & Investment (1 <sup>st</sup> interview)	Ramallah 12-08-99 10:00-12:00
Union Bank for Savings & Investments	Ramallah 12-08-99 12:30-2:30
Cairo Amman Bank	Ramallah 12-09-99 10:00-12:00
Arab Land Bank	Ramallah 12-09-99 12:00-2:00
Palestine International Bank	Ramallah 12-11-99 10:00-12:00
Palestine Investment Bank	Ramallah 12-11-99 12:00-2:00
Arab Bank	Ramallah 12-12-99 10:00-12:00
Arab Palestine Investment Bank	Ramallah 12-13-99 10:00-12:00
The Commercial Bank of Palestine	Ramallah 12-13-99 12:00-2:00
Bank of Jordan	Ramallah 12-14-99 10:00-12:00
Jordan National Bank	Ramallah 12-14-99 12:00-2:00
AL-Aqsa Islamic Bank	Ramallah 12-15-99 10:00-12:00
International Arab Islamic Bank, PLC	Ramallah 12-15-99 12:00-2:00

ry dot 2



The Palestinian National Authority  
The Year 2000 Palestinian National Technical Committee

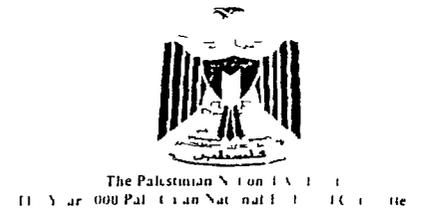
**Y2K Status Presentation with Senior PMA  
Management and Senior Bank Managers at 7PM**

Jordan Gulf Bank	Ramallah	12-16-99	10 00-12 00
Housing Bank	Ramallah	12-16-99	12 00-2 00
Al-Quds Bank for Development & Investment (2 <sup>nd</sup> Interview)	Ramallah	12-18-99	9 15-11 00
Jordan Kuwait Bank	Nablus	12-18-99	12 00-1 30
Bank of Palestine, Ltd	Gaza	12-19-99	9 45-10 45
Palestine Islamic Bank	Gaza	12-19-99	10 55-12 15
The Principal Bank/Egypt	Gaza	12-19-99	12 30-1 15
Visit PMA Headquarters in Gaza for Y2K Review	Gaza	12-19-99	1 20-2 45
Prepare Final Report for PNA PMA Mgmt		12-21/23-99	
Exit Meeting to PMA Governor – Gaza		12-22-99	
Exit Meeting to PMA/PNA Mgmt and USAID		12-23-99	
Submission Final Report to Barents Project Leader		12-24-99	
Submission Final Report to Barents Washington DC Headquarters		12-27-99	



## Bank Officers Met During Review of Banks in Palestine

Bank Name	Date	Time	Names	Job Title
HSBC BANK	12/07/1999	10 00 12 00	Stuart Barkinson Wisam Khouri	Branch Manager Technical Services Clerk
ANZ GRINDLAYS BANK	12/07/1999	12 30 2 30	Anton Batteikha Zafer Abdul- Halim	Executive Manager Technology Officer
Al Quds Bank	12/08/1999	12 30 2 30	Ma'en Al- Labadi Tayseer Oudeh taleb Kifayah Eid Ghayadah Suhail yahya Mohammad Salman Mohammad Fraij	Acting branch manager Branches Operation Manager I T Officer Financial & Administrative Supervisor I T Dep General Manager Head of I T Dept
Union Bank for Saving & Investment	12/08/1999	10 00 12 00	Jamal Zada Musa Shamieh	I S Manager Manager
Cairo Amman Bank	12/09/1999	10 00 12 00	Tayseer Qutteineh Imad Jarallah Waddah Khamlan Mahmoud Al- Ramaah	Executive Manager Bank Op Administrative Manager I T Dept Banking Operation Dept Regional
Arab Land Bank	12/09/1999	12 30 2 30	So'od Dardas Ahed Al-Bakhiet	Financial Manager I T Dep Regional
Palestine International Bank	12/11/1999	10 00 12 00	Usama Khader Kaysar Omar Ammar Khdairy Ghazi Musleh	General Manager Operation Supervisor EDP Manager Deputy General Manager
Palestine Investment Bank	12/11/1999	12 00 1 30	Yousif Al- Qadi Salah Farris	Deputy General Manager I T Dept
Arab Bank	12/12/1999	10 00 12 00	Taysir Khalil E Ahmed Abu-Ghosh Khaled Ghannam	Financial Controller Head of ISC Palestine Manager Supply & Premises Dept
Arab Palestinian Investment Bank	12/13/1999	10 00 12 00	Masoud Al- Ardah Adel Lafi	Director MIS Officer



The Commercial Bank of Palestine	12/13/1999	12 00 2 00	Abdallah Khalil Basem Maraqa Issa Mrebe Sbeih Al- Khalily	Manager I T Dept Branch Manager Al Ram Accounting Dep
Bank of Jordan	12/14/1999	10 00-12 00	Fayez Al Dabbas	Banking Operation Manager
Jordan National Bank	12/14/1999	12 00-2 00	Anwar Jyousi Assaf Bleidi Mahmoud Al Zaben	Assistant R Manager Computer Division Head Financial Controller
Al- Aqsa Islamic Bank	12/15/1999	10 00-12 00	Dr Mohd Sarsour Muhsen Abdl Wahab	Dy General Manager Computer Dept Admin
Arab Islamic Bank	12/15/1999	12 00 2 00	Ayoub Kamal Nabeel Samara Murad Saleh Taghrid Ameireh	Operation Manager Inspection Dept Manager I T Dept Manager Head Office Financial Manager
Jordan Gulf Bank	12/16/1999	10 00 12 00	Izzat Thawabeh Watheq Omar	Facilities & Credit Control Manager I T Dept Manager
Housing Bank of Jo	12/16/1999	12 00-2 00	Dr Anis Al- Hajjeh Mohammed Khaled	Regional Manager I T Dept Manager
Jordan Kuwaiti Bank	12/18/1999	10 30-12 00	Hasan Husein Yousef Mukahhal	Branch Manager Assist Manager
Bank of Palestine LTD	12/19/1999	10 30-12 00	Dr Hani AL Shawa Ihab Al Aloul E Aladdin El Astal Saeb Sammour Bassam Abu Sha ban Samer Nassar	Vice Chairman Deputy G Manager Head of Computer Division Head of Services & Maintenance General Supervisor Assisitant Head of I T Dept West Bank Legal Adviser
Palestine Islamic Bank	12/19/1999	12 00-1 00	Ali Al- Zammar Sameh Al- Bhaisy	Deputy General Manager Head of I T Dept
The Principle Bank for Development & Agricultural Credit	12/19/1999	1 00 2 00	Abbas Abdel Hadi Eid Bshara Naser Audeh	Branch Manager Head of Accounting Dept Head of I T Dept





## **A Message To The Palestinian People From The Palestine Monetary Authority (PMA) About Year 2000 (Y2K)**

### **The Banks & Bank Branches of Palestine Are Well Prepared For Y2K**

#### **Introduction**

The year 2000 compliance issue is a major problem challenging many organizations all over the world. This problem may affect the business sector of our economy seriously, especially the financial sector which is one of the most important sectors in our life. The year 2000 problem which is also called the Millennium Bug is not only a computer problem but is also a business issue. Therefore one of our main concerns at the PMA was to guarantee that the banks and bank branches in Palestine solved it properly so that the Palestinian people could be assured of accurate and efficient banking services in the year 2000 and beyond. At the PMA the year 2000 readiness program has been a high priority since 1998. The PMA has made sure that all banks had teams of people working on this important project. After continuing overview and supervision we at the PMA can assure you that the bank computer equipment, communication networks, operating system software, data bases and application programs have been properly readied and fully tested in every bank in Palestine.

#### **PMA Role Overview and Supervision Role**

The PMA was monitoring, controlling and reviewing the year 2000 projects and preparations being made at every bank in Palestine. The PMA made sure that every bank and branch gave Y2K the highest priority. At this point in time every bank is finished with their Y2K projects and are properly prepared to operate in the new millennium.

#### **Contingency Plans Were Developed**

The PMA made sure that as a part of every bank's preparation included the development of a contingency plan. This plan assures you the Palestinian people, that the banks in Palestine will have business continuity in case there is any problem with the electrical power or telecommunication systems. The risks (of whatever nature or source) to the banking system of Palestine were identified and evaluated by each bank and plans were made to address each one so that the banks will continue to operate for the people.

#### **Banking Holiday on January 2, 2000**

The Governor of the PMA and the Palestinian National Authority have decided to declare Sunday 02-01-2000 as a banking holiday so that all banks will be able to make one final series of tests and checks to be sure every preparation for Y2K is ready and proper. Since this day has also been declared a holiday for neighboring countries (Jordan and Israel) and it is normally a holiday for all of the rest of the banks in the world there will be no harm to the Palestine banks and branches or our economy because of this extra holiday. All banks will be open and ready for business on Monday 03-01-2000.



## Questions and Answers on the Year 2000 Problem

### *How widespread is the Year 2000 problem in the banking industry?*

Any person or organization that uses computerized systems or equipment can be affected by the Year 2000 date change. But banks and savings institutions are among those companies that can be especially affected by the problem. Why? Because so many of the transactions they handle involve date-sensitive information, such as the date that deposits or payments are made, which in turn affects account balances and interest calculations. That's why the financial services industry is taking aggressive steps to make sure its computer systems will process transactions properly in the Year 2000.

### *What is my bank doing to make sure that its systems will work correctly?*

From the smallest to the largest, banks are checking and fixing their computer systems to make sure they will operate smoothly in the Year 2000. Banks and savings institutions are required by federal regulators to have plans in place to get their systems Y2K ready. Each institution's readiness plan is different because it must be tailored to its own situation. Banks are expected to have these crucial steps completed well before the Year 2000.

### *Who's checking to make sure my bank is doing what it needs to do?*

The PMA is closely monitoring the progress of banks in completing the critical steps required by their Year 2000 plans. Thus far, banks are meeting the regulators' expectations.

### *Is there anything I can do to tell if my institution has taken steps to get ready for the Year 2000 date change?*

First, read everything your bank gives you regarding the Year 2000 and its efforts to be Y2K ready. Most institutions expect that their customers will have questions, so they've prepared statement stuffers, brochures, and articles for customer newsletters that describe their Year 2000 readiness efforts. Institutions also are holding Year 2000 seminars to provide information to customers and answer questions. If you call or visit your bank and ask about its plans to get ready for the Year 2000 date change, talk to an employee who is knowledgeable about the institution's Y2K program.

### *How could a Y2K problem affect my banking routine?*

Your daily banking routine generally should not be affected. Despite the banking industry's best efforts, however, some customers could encounter disruptions in service or other problems. To make sure that banks are ready to deal with problems quickly and effectively, all are required to establish plans that will provide for alternative methods of doing business, if needed.

### *How will I know if my account balances are correct after January 1, 2000?*

The best way to verify the accuracy of the transactions posted to your account is to review your bank statement. If



do that you need to have complete and accurate records of all your account transactions—a prudent practice under any circumstances.

We suggest you keep copies of your deposit slips, bank statements and other records of your transactions, especially those for the last six months of 1999 and the first few months of 2000. Compare your records against what's shown on your statement. If you find a discrepancy, contact your institution to resolve the error. When it comes to double-checking the amount of interest credited to your account, trying to do the calculations yourself can be complicated.

Instead, you might want to simply compare the interest shown on your current monthly statement with the amount found on some earlier statements. If the amount doesn't look right, contact your bank or savings institution for help in checking the calculation. Also be aware that institutions are required to keep back-up records for account transactions so they can recover this information in case of an emergency.

These back-up records could be used to identify and correct errors that might affect your deposit, loan or other account due to a Year 2000 computer problem.



## Y2K Fraud Warning for the Citizens of Palestine

### Beware of Y2K scams

The Year 2000 computer problem isn't a problem for criminals -it's an opportunity to cash in on people's fears about the unknown. While chances are you'll never encounter a Y2K con, we want you to know how to spot the warning signs so you won't end up a victim. The Palestine Monetary Authority (PMA) believe that scams such as these could become more prominent in the coming months.

A con artist posing as a bank employee calls to say that as part of a Year 2000 fix of the bank's computers, you must confirm (actually reveal) your credit card or bank account number. The crook then uses this information to order new credit cards or checks in your name and goes on a shopping spree. Never give out account information, credit card or social security numbers, or other personal information to someone you don't know, unless you have initiated the contact. Bank customers should report any suspicious requests for confidential account information.

You receive an unsolicited offer to 'hold' your money until after January 1, 2000, in a place that's supposedly safer than your bank. The money would only go into the crook's pocket.

A sales person from a company you never heard of calls to suggest that you buy into an investment that's free of Year 2000 problems (or will 'solve' Y2K problems) and is guaranteed to net a big profit. It's likely the only one profiting will be the seller, while you get little or nothing in return.

### Best Defenses

The PMA wants you to be Y2K-careful. Here are four things you can do to protect yourself from a potential Y2K swindle.

1. Remember the classic 'red flags' of a financial swindle. We suggest you hang up the phone or walk away from any unsolicited offer if
  - The deal seems too good to be true or doesn't seem to make sense
  - The offer is from an unfamiliar company, often without a street address or direct telephone number
  - The person or company won't give you written details of the offer
  - You're asked to give cash, a check, or your credit card or bank account number before you receive goods or services
  - The sales person uses high pressure tactics or is intimidating
  - Protect your personal financial information
2. Never give out your bank account or credit card numbers to an unknown person or company, unless you initiated the contact, and never give anyone the Personal Identification Number you use to access an ATM. A con artist can use this information to withdraw money from your bank account or order new credit cards in your name.



- 3 Check out any offer to buy or invest in a product or service before you commit to anything. If you're seriously considering an offer, get as much information as you can before you agree to pay money. Always confirm with a reliable source whether you do indeed have a problem or that there isn't a better solution. For example, if you're approached about a supposed Y2K problem with your bank account, independently check with your financial institution.

- 4 Take the time to spot and report a possible fraud.

Always review your account statements and credit card bills to make sure a swindler hasn't withdrawn money or made purchases in your name. Also, if one of these regular mailings doesn't arrive, that could be a sign someone may have changed your billing address for fraudulent purposes. If you think you've been the victim of a scam or just suspect something fishy, call your bank or the police immediately.

If you just remember these four simple steps, it's a good bet that you won't have to worry about being the victim of a Y2K scam.



## Common Sense Rules to Protect Your PC From Viruses

Regardless of your operating system, these six rules should protect you from most of the over 46 000 viruses that are currently floating around the internet

### 1 Purchase A Good, Commercial Antivirus Program Like Norton Antivirus Or McAfee Virus scan

Most commercial antivirus programs usually cost between US\$40 and US\$50 and can be purchased at almost any computer store in the world [You can usually save about US\$10 if you purchase the software online - visit <http://www.shopper.com/> for more information]

Antivirus program manufacturers also release minor upgrades every two to three months and major upgrades every twelve to eighteen months **YOU NEED THESE UPDATES** Minor upgrades are usually free and major upgrades usually cost anywhere between US\$20 and US\$40 depending on the manufacturer [think of this as an expected expense -- just as you have to change your car's oil every 3 000 miles you have to upgrade your antivirus software every year to year and a-half]

To see if any minor or major upgrades are available for your antivirus program visit your antivirus program manufacturer's homepage A list of antivirus manufacturers' homepages can be found at <http://www.yahoo.com/> or at AOL keyword "virus"

### 2 Update Your Virus Definitions Frequently (At Least Once A Week)

With over 250 new viruses being discovered each week if you don't update your definitions frequently you won't be protected from ANY of the new viruses floating around the Net

How do you update your virus definitions? That depends on the antivirus program you use Norton Antivirus has a "Live Update" button built into the program click on it and Norton automatically downloads and installs the latest virus definitions from Net McAfee VirusScan has a similar update function (go to File > Update VirusScan)

If you are unsure of how to update your virus definitions visit the homepage of your antivirus software manufacturer and look for their "download update" or "technical support" section

### 3 Never Double-Click (Or Launch) \* Any \* File, Especially An Email Attachment, Regardless Of Who The File Is From, Until You First Scan That File With Your Antivirus Program



syawab



The Palestinian National Authority  
The Year 000 Palestinian National Technical University

This is probably the most important rule of them all. There are currently over forty-six thousand viruses out there. There are over 2.8 trillion possible file names out there, and any one of those viruses could be hiding in any one of those file names. A lot of people think that you can protect yourself from a computer virus by being on the lookout for one particular virus or one particular file name (hence all of the virus warnings you have received in your email inbox lately). That's not only silly, that's dangerous. If you want to protect your computer from viruses, you need to ignore ALL of the virus warnings you receive and instead be wary of EVERY file you see, especially every file that is attached to an email message.

It is important to note that, despite all of the warnings to the contrary, there is no such thing as an email virus. If you are running the most up-to-date version of Windows (see rule #5 below) or if you have a Mac, you can open your emails, regardless of their subject lines, without fear of infecting your computer, provided your email program doesn't automatically open attachments (most don't). It is the files that are ATTACHED to emails that you have to fear. Think of a computer virus as a well-packaged letter bomb. You can move a letter bomb from room to room in your house without any danger. Open the letter bomb, however, and you die. The same is true with computer viruses. You could download a billion virus-infected files from the Internet and receive another billion virus-infected files attached to email messages and your computer still couldn't be infected with a virus. Open or double-click on just ONE of those files, though, and your computer is dead.

Remember, to infect your computer with a virus, you have to open (or double-click on) a file that contains a virus. As long as you don't open that file, you really have nothing to fear.

How can you scan a file for viruses? It depends on the antivirus program you use. The best bet is to read your antivirus program's instructions or read its online help section. If you use Norton Antivirus or McAfee VirusScan, right-click (or, if you have a Mac, click and hold) on the file in question. A pop-up menu should appear, and one of the choices should be "Scan with..." and the name of your antivirus program. If that doesn't work, just open your antivirus program and try to scan the file from there.

Do you have to scan EVERY file, even if that file is from your friends or coworkers? Yes! Both the Melissa and the WormExplore Zip viruses distributed themselves by opening your email program, looking at either your "friends" list or the list of email addresses in your inbox, and then distributing virus-infected files to everyone on that list.

In the world of computer viruses, you can't trust ANYONE.

---

#### **4 Turn On Macro Virus Protection In Microsoft Word, And Beware Of All Word Macros Especially If You Don't Know What Macros Are**

---

Word Macros are saved sequences of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. They enable advanced Word users to easily accomplish what would otherwise be difficult tasks. They also allow virus writers to do serious damage to your computer. For example, the Melissa virus was actually a Word Macro virus.



If you use Word 97 go to Tools --> Options. Click on the "General" tab. Make sure that "Macro virus protection" (at the bottom of the list) is checked. If you use Word 2000 Double-click on the Tools menu point to "Macro" and then choose "Security". Select the level of security you want. High security will allow only macros that have been signed to open. Unsigned macros will be automatically disabled. Low security always brings up the macro dialog protection box that allows you to disable macros if you are in the middle of the macros.

With Macro virus protection turned on Microsoft Word will warn you every time you try to open a Word document that contains a macro. The warning gives you three choices: the option to open the file but disable its macros ("disable macros"), open the file with macros enabled ("enable macros") or the option to not open the file ("do not open"). Choose the first (default) option "disable macros".

For more information visit the Macro Virus Protection page at <http://officeupdate.microsoft.com/focus/articles/097mcrd.htm>

---

## 5 Run Windows Update At Least Once A Month

---

Windows is aptly named because it is full of holes. There are several 'inadvertent open doors' (or security holes) in the Windows operating system that \*COULD\* conceivably make your computer vulnerable to outside attack. In specific a mean-spirited hacker \*COULD\* walk through one of these open doors on your Windows PC and read any file on your computer, delete specific files or programs, or even completely erase your hard drive.

When the folks at Microsoft discover a security hole they immediately release a software patch to close it. Without the patch - and there are MANY - your computer is wide open to outside attack.

Fortunately downloading these patches couldn't be simpler. Built into every Windows 95 and Windows 98 PC is something called 'Windows Update'. Windows Update is completely free, but there is one catch: you have to have Internet Explorer 5 to be able to use it. (Here is how to use Windows Update to download all of the security patches Microsoft has released since your PC was made.)

1. Connect (or logon) to the Internet.
2. Go to Start --> Settings --> Windows Update on your PC. This launches Internet Explorer and connects you to Microsoft's Windows Update page [ <http://windowupdate.microsoft.com/> ]. If you don't have Internet Explorer 5 (IE5), Microsoft's Windows Update page will talk you through the process of downloading IE5. If you already have IE5, keep reading.
3. On the top left-hand side of the Windows Update page, click on the "Product Updates" link (it is the one with the hand and the red \*).
4. A pop up window will appear, telling you to wait while your computer DOESN'T send any information to Microsoft (well, that's what it says!)



Eventually you'll see a page that says 'Select Software'. When Microsoft releases an essential update or patch to close a security hole in Windows, they put it in this page's "Critical Updates" section. Select (or click on) EVERYTHING in the Critical Updates section -- you need \*ALL\* of the critical updates -- and then click on the big gray "Download" arrow in the top right hand corner of the page.

Follow the on-screen prompts. That's it! New security holes are found in Windows every week or two, so it is a good idea to run Windows Update at least once a month. The first time you run it, expect to see a MESS of critical updates. After that, though, there should only be one or two critical updates you'll have to download every month.

---

## 6. If Someone Unexpectedly Sends You An Executable File -- In Other Words, A File That Ends In .exe -- Throw It Out

---

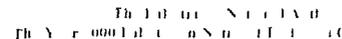
Most of the forty-six thousand viruses that are floating around the Net right now are hiding in executable files. If someone, even a close personal friend, unexpectedly sends you a file that ends in .exe -- or if they unexpectedly send you a zipped file that contains a file or files that end in .exe -- your safest bet is to delete the file without opening it.

The key word here is "unexpectedly". If you are expecting a friend to send you an executable file, you certainly don't need to delete that file -- just virus scan it first before you open it.

However, if you are in an environment (like a home) where you don't often receive ANY files attached to your incoming email messages, a better rule would be "When in doubt, throw it out -- and doubt EVERYTHING."

How well will these six rules protect your computer from becoming infected with a virus, Trojan horse, or worm? Take a look at the following questions and decide for yourself: How many people whose computers were infected with the Melissa virus ignored at least one of these rules? ALL OF THEM! How many people who followed these six rules had their computers infected by Melissa? NONE OF THEM! How many people whose computers were infected with the WormExplore Zip virus ignored at least one of these rules? ALL OF THEM! How many people who followed these six rules had their computers infected by the WormExplore Zip virus? NONE OF THEM!

These six rules will not protect you from every computer virus, Trojan horse, or worm, but they will so significantly decrease your computer's chances of becoming infected that you can all but forget about the next virus scare and all the ones that will follow.



## Practical Hints on Y2K for the General Public

As we approach the new millennium here are some common sense suggestions as to how to best prepare for any Y2K related problems. It is possible that we will experience local power outages, some telecommunication problems. In general we do not anticipate any major problems in Palestine, but we encourage you to be prepared for any eventualities.

In an effort to help you prepare for Y2K, here are some helpful tips for risk reduction prior to January 1, 2000. This document is organized into sections comprising the possible primary failure points of national or local infrastructure should Y2K-related problems occur in Palestine. Each section contains a short discussion of the probability and nature of failures as well as some guidelines to consider when preparing your home and family for potential Y2K problems. When possible, care has been taken to recommend the most economical, safe, and effective means to reduce risk for a household. That is, many of the risk reduction measures do not call for exotic equipment or material that a household would not require over time anyway.

### Power

Although a serious loss of power following January 1 is not anticipated, taking a few precautions makes sense. If a loss of power at home will affect each individual slightly differently. However, in general, the loss of power could affect one in the following ways:

**Risk:** Loss of lighting

**Risk Reduction Measure:** Flashlights and extra batteries, battery-powered lanterns (candles or gas powered lanterns are not recommended for safety reasons)

**Risk:** Loss of appliances--not just refrigerator, washer, and dryer (e.g., electric alarm, electric can openers may not function for canned goods, and your hair dryer may not work)

**Risk Reduction Measure:** Manual appliances for food preparation (can openers, etc.). Use bathtubs, sink, or plastic tubs for the wash. Clotheslines and clothespins. Storage containers for products that need freezing or refrigeration and can be kept outside or in an unheated place. Manual alarm clock.

**Risk:** Inability to prepare food

**Risk Reduction Measure:** Stock up on canned foods, cereals, and other ready-to-eat goods. Prepare meals in advance and freeze. Boxed milk has a long shelf life. Obtain a small grill (use outdoors only), charcoal, and lighter fluid.

**Risk:** Automatic garage doors or gates may not function

**Risk Reduction Measure:** Try to operate all automatic doors and gates without the remote. If all else fails, park your car outside.

**Risk:** Loss of radio/television to get information on the problem

**Risk Reduction Measure:** Obtain battery-powered radio

**Risk:** Loss of alarm system

**Risk Reduction Measure:** Ensure house is locked at all times

1 of 20 + 7



**Risk** No fuel supply at local gas station

**Risk Reduction Measure** Fill up vehicle prior to 1/1/2000 Use only when necessary afterwards

**Risk** Loss of hard-wired smoke alarms

**Risk Reduction Measure** If your smoke alarms are not powered by batteries obtain battery operated alarms

**Risk** Loss of natural gas supply to house

**Risk Reduction Measure** If your house is gas heated ensure that you have adequate layers of winter clothing and extra blankets on hand The whole family could sleep in one room to conserve body heat and monitor children Do not use gas fueled heating appliances indoors You might not have hot water in this situation Consider moving to a friend's heated quarters Use fireplaces if they function well Stock up on wood

**Risk** No pump/heating circulation

**Risk Reduction Measure** As above only this also means you will have no hot water either

## Telecommunications

While a lengthy loss of telecommunications is not likely it is prudent to be prepared Obtaining a cellular phone is recommended Cell phone service providers are confident of the system working However the circuits may be jammed with all the calls going through in an emergency situation

## Finance

Most banks indicate that they are fully Y2K compliant However there is no guarantee that problems transmitted through international commerce won't affect currently compliant systems Caution related to Y2K could lead individuals to hold larger than usual amounts of cash with last minute demand for cash an eventuality for which banks are preparing

**Risk** Inability to get cash

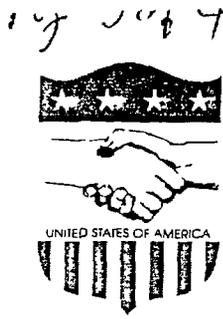
**Risk Reduction Measure** You may want to have enough cash to last for at least one week (about one week's total normal expenses) mixed Your cash reserve should be obtained early should you deem it necessary

**Risk** Financial computer systems go down causing a loss of data Incorrect calculations occur financial transfers and automatic payments fail your account balance is misrepresented

**Risk Reduction Measure** Ensure you have the most recent statements in hard copy Obtain hard copy proof of financial holdings including mutual funds and brokerage accounts deeds to real estate mortgage documentation credit card statements Automatic payment of mortgages and/or other bills may not function

**Risk** Insurance systems encounter problems

**Risk Reduction Measure** Review insurance policies and ensure all documentation including payments records are on hand be sure to check life auto health and property policies Carry health card with you (there might not be a way to confirm benefits should difficulties arise)



**Risk** ATM failures and inability to use credit cards

**Risk Reduction Measure** Obtain cash well in advance, store it in a secure place. Remember thieves read Y2K tips too

## Healthcare Systems

This is an area of some concern to many experts. Because healthcare systems are dependent on so many other sectors, the opportunity for Y2K failure due to dependency on power, telecommunications and water must be considered. Advanced life support systems have a possibility of malfunctioning if older (pre-1997) microprocessors are in the system.

**Risk** Inability to obtain medication due to supply or prescription system failure

**Risk Reduction Measure** Individuals requiring medication through the months of January and February should attempt to stock up in advance. See your doctor for advice on quantities and storage requirements.

**Risk** Loss of power jeopardizes storage of medication

**Risk Reduction Measure** See your medical specialist for handling of medication without refrigeration. Individual or family members with chronic condition may be in jeopardy due to failure of critical care equipment. See your doctor now to discuss your situation.

**Risk** Medical information systems fail, losing data on your medical history and/or insurance information

**Risk Reduction Measure** Ensure you have the most complete set of medical records available. Obtain a copy of your medical insurance card and policy.

## Water and Wastewater

The prudent individual will stock up on bottled water, perhaps as much as a two week supply. One rule of thumb to calculate the amount required can be one gallon per person per day. (This rule is based on a single person; for families, decrease the requirement in proportion to the size of the family. For example, a couple might need 15 gallons per day (7.5 gallons per person). A family of seven might only need 4 gallons per day (6 gallons per person). Old water bottles can be filled with tap water through the end of the year to be used for bathing, washing and flushing requirements. Distilled water can also be stored. Instructions on the correct procedures for storing distilled water can be obtained from health authorities.

## Public Services

Police, fire and ambulance service could be affected if dispatching equipment and telecommunications break down.

Trash removal, road maintenance and septic tank maintenance services are unlikely to break down, but might be affected in the longer term if gas supplies become a problem. Please take extra precautions with safety and security.

## Transportation

Bus systems are expected to work as normal through the New Year period. Travel in the region and international through this period may be problematic in some cases given the uncertainties associated with Y2K.



The Palestinian National Authority  
The Year 2000 Palestinian National Technical Committee

While some vehicles may experience Y2K-related problems, manufacturers anticipate that there are few safety problems associated with them. The following guidelines should be used in the event of a Y2K-related failure:

When driving, be aware that traffic lights might be affected by loss of power as will street lighting.

Most authorities say air travel should not be dangerous during the Y2K period. It appears that the most susceptible elements of the airlines are the ticketing and scheduling systems. Delays caused by malfunctions could inconvenience travelers worldwide. These malfunctions should be known on January 1st or shortly afterward. Fuel and repair part supplies could be a problem later in certain countries, causing delays and cancellations.



## PRESS RELEASE FROM PMA DEC-16-99 (PAGE 1 OF 2)

### **Beseiso Assures Palestinians that the Banking Sector is Y2K Compliant and He Will Set Up an Emergency PMA Committee to Manage this Process**

Dr. Beseiso, the governor of the Palestine Monetary Authority (PMA) confirmed that the banks preparedness for Y2K is good and he declared he was formulating an emergency committee where PMA will work with all Palestinian banks to track and manage this issue over the last few weeks of this millennium and the first few weeks of the new millennium.

The PMA held a meeting yesterday which was organized by the Palestinian Institute for Banking and Financial Studies. The meeting was led by Dr. Fouad Beseiso, Governor of the PMA. Representatives from all Palestinian banks were present. In most cases, the bank's general or regional managers and many of their senior IT Managers participated. There were also representatives from PNA ministries and experts from the USAID.

Dr. Beseiso stated at the beginning of the meeting that he has sponsored a final review of all Palestinian banks preparedness for their Year 2000 conversion into the new millennium.

He indicated also that the USAID as a donor agency to the PNA and PMA has sponsored Mr. Richard Sticher, an Information Technology (IT) and Y2K Expert to evaluate the preparatory Y2K process at the PMA and to visit and review the Y2K situation for all of the banks in Palestine.

About his impression, Dr. Beseiso assured the participants at the meeting that the banks preparedness is good and he said we are here to review the summary findings and conclusions presented by the IT Expert. From the other side, Mr. Richard Sticher spoke about the Y2K issue and its international impacts. He reviewed the progress in preparing for the Y2K millennium date change and spoke about the large sums of money that has been spent throughout the world on these projects.

He stated that there had been a level of global cooperation between countries, governments and business to assist each other in their Y2K preparations to a level that has never before been seen. He said that cooperation was high throughout the world as the millennium closes to an end. He said that it affects all sectors of our lives and that the telecommunication and energy sectors did the best for solving the problem and the health sector could be the most negatively affected sector in this part of the world.

He stated that in a recent survey by experts that the level of readiness in the two neighboring countries adjacent to Palestine (Israel and Jordan) was high and that there had been a very high level of cooperation between the banks and Central banks in these two countries with our banks. He said that with the strong efforts of every Palestinian bank and with the help from our neighbors, the banking sector of our economy should not have major Y2K related issues or problems.

Mr. Sticher clarified that he had visited 15 Palestinian banks so far and that he would visit the last 6 over the next few days in order to finish his review of all banks for the PMA.



## **PRESS RELEASE FROM PMA DEC-16-99 (PAGE 2 OF 2)**

He spoke about what the PMA's role had been in monitoring and supporting the banks in the development of their procedures. They monitored the banks' progress so that the \$2k transition would be positive and that the banks would be ready and prepared.

After the presentation a general question and answer discussion was held with the bankers and others present. Numerous questions about \$2k were raised and answered by Mr. Stichter.

**Press Release by PMA to the AL-HAYAT AL-JADIDA, Jerusalem and AL-AYAM  
Newspapers on December 16, 1998**



The Palestinian National Authority  
The Year 2000 Technical National Technical Committee

Name	Organization	Title	Telephone Number	Fax Number	E-mail Address
Dr. Ghassan Z. Qadahi	Government Computer Center	Supervisor General to The Government Computer Center	2961866	2961865	qadahi@hally.net
Nizam Mohammed Hammad Harb	Palestinian Central Bureau of Statistics	Director General Information systems & computer	2406340	2406343	nharb@pcbs.pna.org
Omar Doud Jameel Alshihli	PECDAR Palestinian Economic Council for Development & Reconstruction	Director Information Technology Dept	2362300 2362357	2347041	osahili@pecdar.pna.net
Laysar Ahmad Ibrahim Idreis	Ministry Of Local Government	Program Coordinator	2402345 2402346 2402347 050220972	2402349	mlg@plmnet.edu
Imad Ahmed Mosa Younis	Government Computer Center	Year 2000 Technical Project Manager (West Bank Coordinator)	2961866	2961865	imadyounis@yahoo.com
Rami Mohammed Ahmed Samirith	Palestinian Monetary Authority	System Analyst	2959920	2959922	smrmita@pma.com.pn.net
Hisham Ibrahim Mohammed Omar	Jerusalem Electric Company Palestinian Energy Authority	Planning Manager	6282333	6282441	hjdccot@pea.com
Bishar Fouad Bishara Khouri	Government Computer Center	Director General / Ministerial Advisor	2829262	2863900	bishara@yahoo.com
Usamah Mohammed Ismael Madhoum	Ministry of Post and Telecommunication	Director General Systems and Information Dept (Gaza Coordinator)	2826226	2822222	cladabou@palnet.com
Mahmoud Ali Mohammed Al Haj	Ministry of Finance	Director System and Information Dept	2835772	2825964	finance@hally.net
Nizam Mahmoud Ali Muhsin	Ministry of Health	Director Computer and Telecommunication Dept	2822969 2827721	2864109	mohite@hally.net
Howaidi Ahmed Mohammed AbulHuwaidi	Gaza City Municipality		2866006	2824400	howaidi@hotmail.com
Saudi Zuhdi Ibrahim Abu Trab	Ministry of Housing	Deputy Manager Computer Dept	2822233 2833483	2822233 2822665	rtnta@hotmail.com

**Gathering Year 2000 Information from  
Financial Institutions:  
Recommendations for Supervisors**

**Basel Committee on Banking Supervision**

Basel  
September 1999

## **Gathering Year 2000 Information from Financial Institutions: Recommendations for Supervisors**

### **Overview**

This document recommends an approach for supervisors to use in gathering reliable information from their financial institutions in a timely and efficient fashion during the Year 2000 rollover period. The successful implementation of this approach requires that it be properly planned and tested before the Year 2000 event takes place.

Supervisors will need to be well informed during the rollover period to identify internal and external problems that could disrupt financial institutions and markets and to dispel misinformation. There will also be heavy demand for information on progress not only from other supervisors and national coordinators but also from customers and counterparties of financial institutions, and from the general public. Gathering and disseminating accurate information on the Year 2000 rollover in a timely manner will therefore be a priority for banks and their supervisors.

The approach put forward recognises that clear expectations for information flows between the private and public sector are essential for efficient communications. Although needs will vary among the various parties and as specific situations unfold, advance agreement on a minimal set of very basic information will avoid redundant, inefficient communication links and information gathering. For stand-alone entities or head offices there may well be a need for more detailed and intensive reporting arrangements, though these would not be mandatory. For globally active institutions, reporting can be minimised if normal relationships are maintained between the local supervisors and institutions they regulate. When any material problem is identified, more detailed information specific to the particular circumstances can be sought.

This approach is flexible. It does not suggest a standard form for the financial institution to complete. While some supervisors may not want to use a form, others will.

### **Recommendations for Supervisors**

#### **1 Reporting Efficiency**

Obtaining information efficiently requires a careful balancing of the need for information and the burden for developing and collecting the information. A paper being released simultaneously with this one develops guidance for supervisory information sharing<sup>1</sup>. This

---

<sup>1</sup> *Year 2000 Cross Border Communications between Supervisors during the Millennium Period*

paper suggests four basic principles for communication strategies during the Year 2000 rollover period These principles are

- Keep communications as simple as possible
- Focus on material issues
- Leverage off existing information flows, existing groups, and work being done by others to develop communication links<sup>2</sup>
- Define communication responsibilities in advance

These same principles apply in developing strategies for collecting information from financial institutions The attached annex extends these principles more specifically to such information-gathering

**2 Exception Reporting**

The primary need for supervisors will be exception reporting<sup>3</sup> of problems encountered by financial institutions Supervisors should therefore take steps to ensure that Year 2000 problems which pose material risks<sup>4</sup> for the normal conduct of business and prudential health are identified and reported to supervisors as soon as they are identified

**3 Status Reports**

Most supervisors will want to consider instituting some type of supplemental information-gathering on whether the financial institutions and the supporting infrastructure are ready for business and are expected to operate normally In collecting supplemental information, supervisors need to recognise that information gathering processes can divert scarce resources from the first priority of financial institutions, which will be to identify and fix any problems that may arise

---

<sup>2</sup> This paper should be read in concert with the work that the Joint Year 2000 Council and the Global 2000 Coordinating Group are currently doing on information sharing It is the intent of this note that it complements the work of these groups

<sup>3</sup> Problems are encountered every day in the normal course of business For Year 2000 purposes it may be useful to distinguish this normal level of problems from Year 2000 ones by considering a scale of potential disruptions 1) operating normally 2) some partial or intermittent disruptions 3) significant disruptions and 4) unable to operate

<sup>4</sup> Materiality is always a difficult concept to define especially when related to operational events or issues and for different organisations and circumstances Examples of Year 2000 events that may be regarded as material are a shutdown of significant business production or product delivery operations significant interruption of internal risk management or information processes considerable revenue loss or the probability of a significant litigation expense and significant reputational risk

#### 4 Information Gathering Methods

Information from financial institutions may be gathered in a variety of ways. Under normal circumstances, supervisors collect information using a combination of structured reports, on site reviews, and telephone inquiries. Each approach has its advantages and limitations. For information with a short time life, structured reports often are more difficult to compile but easier to analyse, while less structured approaches simplify the information-gathering process but often make the analysis more difficult. The relative burden and benefit of the alternative approaches for information gathering to both the reporting institution and the supervisor should be considered.<sup>5</sup> Whatever method is used, supervisors need to be confident that the information received is accurate and reliable.

#### 5 Basic Information

However gathered, status information should be kept as simple as possible and focus on five basic questions:

- Is the Year 2000 rollover proceeding satisfactorily to allow the *normal conduct of business*?
- Are there *material internal problems* affecting the core businesses?
- Are there *external issues* affecting the ability to do business?
- If there are problems encountered, is the core business nonetheless able to keep functioning by making *use of business contingency plans*?
- Are there *other factors* such as market conditions or rumours materially affecting the business?

If the answers to these questions indicate no difficulties, the inquiry can effectively end in most instances.<sup>7</sup> If any of these answers elicits supervisory concerns, further inquiries are appropriate to obtain more detailed information on the business lines/entities affected, the contingency and problem resolution measures being put in place or considered, and the expected duration of the problem.

---

<sup>5</sup> Supervisory personnel often complete structured reports using information gathered through less structured contacts. Where accountability is sought, a more structured approach to reporting may be appropriate, including sign-offs by senior officials – providing such sign-offs do not risk impeding both the timeliness and/or the candour of the information provided.

<sup>6</sup> Note that Year 2000 problems encountered as a result of testing over the event weekend may be capable of being fixed without any adverse effect on normal business activity on the first business day.

Stopping the information gathering process at this point applies equally to both structured reports and to less structured forms of communication.

## 6 Timing

Supervisors need to recognise that information needs will change during the rollover period and design the timing of their information gathering activities accordingly. In general there are three basic time periods:

- *The period immediately after the date change* up until the normal opening of business on the first business day. During this period information needs will focus on testing of systems to assure readiness for the normal opening of business and issues with the infrastructure or other external dependencies<sup>8</sup>
- *The first business day*. During this period the focus will be on whether systems are operating normally and whether any unusual market behaviours are being noted.
- *From the close of the first business day* including the successful completion of overnight processing. If problems are encountered the duration of this third period may be extended to ensure that all problems are resolved.

Exception reporting for material matters will be necessary throughout all three periods. Status information should be gathered at frequencies at the supervisors' discretion. In order to monitor market conditions the greatest need for information may occur on the first business day. Different criteria may be appropriate for status information from large and small financial institutions depending on their potential systemic impact.

---

<sup>8</sup> Information needs will also focus on 24 hour retail business such as ATM/POS performance.

## Y2K Rollover Principles for Supervisory Information Gathering

Application by supervisors of the following principles will help ensure that the collection and use of information by supervisors is as efficient as possible from the point of view of both supervisors and supervised institutions. This in turn will help both to concentrate on achieving adequate business continuity over the event period without having to commit disproportionate resources to information gathering and management. Although the principles have been developed by bank supervisors, the Basel Committee considers that they have general relevance to reporting by securities and insurance market participants and potentially other market participants.

In all cases, it is key to keep in mind the following principles and to attempt to limit the flow of information to only what is absolutely necessary or essential to address the supervisory issues that may surface.

- 1 Information demands should be *prioritised* according to impact, risk and materiality.
- 2 The *timing and content* of supervisors' information demands should not risk distorting firms' own event management timetables.
- 3 Supervisors should be interested primarily in *readiness for opening*. They should not seek to track in detail firms' progress.
- 4 Supervisors' principal requirement should be for *prompt and open notification* (through exception reporting) by financial institutions of material problems either in progress towards readiness for business or in live operation (and a rapid indication of the possible impact and duration of the problem).
- 5 Supervisors may require larger institutions to provide not only exception reports but *status reports at specified times*; in so doing they should give full weight to institutions' need to focus on their rollover tasks in a timely manner.
- 6 Supervisors should so far as possible *limit requests* for detailed information to *exceptions*, and then only so far as necessary to assess and act on the implications of the exception.
- 7 In considering *materiality* and in monitoring progress over the event period, supervisors should take into account that firms typically have New Year bugs every year that in the course of preparing for opening for business, firms may well run into minor Year 2000 bugs which they are well able to fix in good time, and that firms may experience some slippage in their own event timetables without threatening failure to achieve readiness in good time for opening for business.

In providing information on the macro status of the financial sector or the country more generally, care must be taken to provide information in a timely manner and in a balanced way to avoid over-reaction. This is especially true because some problems will almost certainly occur - a blanket 'everything is fine' statement will often lack credibility if there are

10/1/08

even a few known problems in relatively unimportant areas. Similarly the failure to provide any information may well be interpreted in a way that will magnify any problem and add credibility to any rumours that may develop.

**Year 2000 Cross-Border Communications  
between Supervisors during the  
Millennium Period**

**Basel Committee on Banking Supervision**

Basel  
September 1999

## Year 2000 Cross-Border Communications between Supervisors during the Millennium Period

Today's global financial markets require cooperation and close coordination among bank supervisors both within countries and across borders. Such coordination will be especially important in the remaining months of 1999 and early 2000 as banking organisations and markets deal with the Year 2000 challenge.

Unlike most challenges faced by bank supervisors, the Year 2000 is a known and time certain event. Although excellent work is being done to avoid serious problems, almost everyone recognises that some problems will develop. Prudent contingency planning suggests that designing and testing channels for communicating information on Year 2000 matters can be beneficial in many ways. In particular, it can (i) promote the public confidence necessary for stable markets, (ii) lead to greater efficiencies and more accurate information during the period of the date change, and (iii) provide for more efficient resolution of any problems that may develop.

This note outlines an approach that bank supervisors<sup>1</sup> may want to consider as they develop their national and cross-border Year 2000 event management and communication strategies. Four principles are central to the suggested approach:

- **Keep communications as simple as possible**

The demand for information before, during, and immediately after the date change will be tremendous. Although needs may vary among the various parties and the specific situations that unfold, advance agreement on a minimal set of very basic information that will be needed to identify problem areas will avoid redundant, inefficient communication links. Once an issue is identified, more detailed information can be sought specific to the particular circumstances.

- **Focus on material issues**

Examples of what might be designated by supervisors as material events include:

- A shutdown of business, production, or product delivery operations
- Significant interruption of internal risk management or information processes

---

<sup>1</sup> Recognition is given to the fact that bank supervisors need to coordinate their communication strategies with insurance and securities supervisors, taking into account the multi-regulatory environment that many major cross-border financial institutions operate in. In addition, these strategies will need to be shared with central banks and operators of payment systems having a direct impact on banking operations.

10/30/98

- Considerable revenue loss or the probability of a significant litigation expense
- Significant reputational risk
- **Leverage off existing information flows, existing groups, and work being done by others to develop communication links**

Existing groups like the Basel Committee on Banking Supervision, the Executive Meeting of East Asia and Pacific Working Group on Banking Supervision, and the Association of Supervisors of Banks of the Americas and their various working groups have a long history of working cooperatively on difficult cross-border issues. Using groups such as these to communicate on Year 2000 issues provides a level of trust that helps ensure that information will move efficiently and accurately. Where new channels of communication are needed necessary for Year 2000, these channels need to be identified well in advance and procedures for communication developed to instill quality control on information being provided.

- **Define communication responsibilities in advance**

The date certain nature of Year 2000 offers a unique opportunity to plan for a more structured and efficient way to handle communications on all levels. What type of information will be needed and when it should be provided can be defined in advance. Who provides the information and to whom it is provided can also be agreed upon. Additionally, the process for communicating the information in a timely and efficient way can be developed cooperatively. By addressing the information needs, the parties having access, and the processes for sharing information in advance, sharing of critical Year 2000 information during the event rollover period can be greatly enhanced.

### **Gathering Information**

Information sharing protocols of a general or conceptual nature are useful to facilitate initial discussion of cross-border arrangements. However, one of the first responsibilities of any group developing plans to communicate on Year 2000 issues must be to define the specific flows, the content of the flows, and the party responsible for each aspect of the flow. This needs to be done as soon as possible and well before the end of the year.

The suggested approach for effective cross-border communications for the bank supervisors has several key components:

---

Regional groups of bank supervisors provide yet another level of trusted parties with a history of working together on issues of mutual interest. Additionally, this paper should be read in concert with the work that the Joint Year 2000 Council and the Global 2000 Coordinating Group are currently doing on information sharing. It is the intent of this note that it complements the work of all of these groups.

In many cases, as discussed below, the definition of content will be more conceptual in nature rather than a list of specific items because the specific information needs will be shaped by the nature of issues as they are encountered.

1 of 4 of 3

- I It identifies protocols for communications and issue resolution that escalate issues in a predetermined fashion
- II It builds on existing principles for cross-border communication and cooperation. The paradox of needing to disseminate information widely and the general reluctance to share information of a negative nature is addressed
- III It discusses the process that needs to be established over the remaining months of 1999 to ensure that cross-border communications can occur effectively

## I A Hierarchy for Communication and Issue Resolution<sup>4</sup>

### Bilateral Communications

If problems arise concerning an individual bank or banking groups, it is very probable that the supervisors will only wish to discuss them in detail with trusted partners who are directly affected. Such bilateral issue resolution will be in many ways business as usual activities. Accurate identification of normal bilateral contact points -- that is specific information on how trusted contacts can be reached around the date change -- will be essential. In many cases, supervisors are setting up Year 2000 event management communication centres where a variety of people will collect, often on a 24-hour basis, information from different institutions and markets. If this approach is used, special efforts need to be made to ensure that the experts on specific issues will be talking to each other. Since it is likely that in bilateral contacts confidential information will be shared, it is recommended that, before the end of the year, opportunities be sought to test communications channels, get to know each other and develop mutual trust. Without such contact, the level of information exchange is likely to be hampered. In addition, key decision-makers should be available at all times and reachable through contact points, which may become facilitators for bilateral conversations conducted at higher levels.

While contact lists may be developed and shared within existing or newly formed groups, individuals on the lists may want to contact each other bilaterally no later than in early December to develop personal protocols for dealing with each other. Such contacts can also be helpful in agreeing in advance on how certain types of information will be shared between organisations. While it is expected that most bilateral communication will occur on an exception basis, the possibility of scheduling specific conversations during the period between supervisors that have mutual areas of common interest might be considered.

---

<sup>4</sup> In order to facilitate communications between the private and public sector as well as within the public sector, a common terminology as developed by the Global 2000 Coordinating Group is used. While the specific needs of each for cross-border communication will differ, the logic of escalating communications in the way suggested seems to be equally applicable.

<sup>5</sup> One approach being considered by many organisations is a central contact point and call back procedure. While the contact point is publicly available, the call back is between two parties that have been identified in advance as appropriate bilateral contacts. If something like this approach is used, it may mean that individual contact lists are agreed upon bilaterally and not published more generally.

19 07 '95

In a few cases it may be appropriate to pre-schedule bilateral general status conversations between supervisors who share mutual information needs and require positive confirmations of Year 2000 readiness to permit general feedback to the markets. Typically, these conversations would focus on the largest institutions and be timed after local status updates have been conducted.

### **Multilateral Communications**

Multilateral communications will likely occur between organisations that are already networked on a bilateral basis. Effective communication on Year 2000 issues at this level requires consideration of two factors: efficiency and openness of discussion. To address the efficiency issue, specific opportunities for multilateral communication can be established in advance for the event period in order to avoid having to make such arrangements on an *ad hoc* basis.

Exactly who will participate, when (and how) the communication will occur, and the expected content of the communication need to be established in advance. The larger the group, the less likely that sensitive issues will be raised. Leveraging off existing groups of people that routinely work together may be the most effective way to conduct such communications. In many instances, pre-arranged multilateral communications may be limited to situations where a supervisor provides macro views of current status while avoiding any mention of individual organisations.

The Joint Year 2000 Council Secretariat plans to help facilitate and support cross-border exchanges of information among key financial market authorities during the transition period by setting up an information-sharing platform which would provide various services. The central services include maintaining up-to-date contact lists, collecting and disseminating information on the operational status of core infrastructure components, enabling financial market authorities to announce emerging developments and facilitating the organisation of conference calls.

## **II Information Sharing Mechanisms**

Existing supervisory groups will rarely be constituted in a way that can address and resolve a particular issue most effectively. Instead, an *ad hoc* group drawn from one or more of the existing groups with multilateral communication structures and strong internal bilateral relationships will likely become the 'working level' to address issues. Again, good information on how key people can be reached during the period is essential. *Ad hoc* groups formed to address specific issues may also want to take advantage of pre-established multilateral communication opportunities to report on the status of their issue resolution.

Bank supervisors need to ensure in advance that there is agreement about their respective roles and responsibilities in a cross-border context, both for information sharing and for decision-making. Over the years, the Basel Committee and other regional bank supervisory

1998

groups have developed a structure for sharing of information on globally active organisations based on the concept of home and host country responsibilities and the need to protect confidential information. In June 1998, the Basel Committee issued specific guidance on sharing Year 2000 information.<sup>6</sup> To assist in the information sharing mechanisms, the Basel Committee will be requesting supervisors to provide updated information on the contact list issued with the June 1998 guidance. While that guidance focused on the tracking of Year 2000 preparations, the same basic principles for information sharing should carry over into the date change event itself.

### The Roles of Home and Host Supervisors

Home supervisors of a financial institution should be responsible for information and issues relating to the status of the institution and its group, not only as regards its activities in the home market but as a whole. Home country supervisors do not generally provide status information on individual institutions. However, during the date change period they should consider providing cross-market views of the financial sector to foster public confidence and/or to promote accurate understanding of overall conditions in order to help develop sound solutions to any problems that may develop. Such cross-market views are likely to be macro in nature and not deal with issues affecting only specific institutions. Additionally, home country supervisors should facilitate access to Year 2000 information on the infrastructure supporting the financial sector and the country's status more generally. This may be done most effectively by either providing links to national communications centres or by providing periodic summaries during the date change period.

Host country supervisors should focus on the operations affecting their local market. Host supervisors should limit their information requirements to those entities and (to a greater extent than normal) branches which are material to their responsibilities and to their local market. Where head office support of remote operations is critical for the local markets, information on normal functioning of these activities should generally be obtained through the local offices and in less detail than might be provided to the home country supervisor by the head office.<sup>7</sup> To the extent that host country supervisors identify Year 2000 issues for a foreign bank operating in their market, they should contact the home country supervisor regarding the problem on a bilateral basis and work together in resolving it.

Understanding in advance how such communications will be handled in individual countries will help assure that information shared across borders will be accurate and timely.

---

<sup>6</sup> *Supervisory Coordination on Year 2000 Cross border Issues*, Basel Committee, June 1998.

<sup>7</sup> For global institutions that are key players in two or more markets, it may be helpful to reach jointly agreement on how cross border contacts will be handled on issues affecting a particular firm, country or market. Confirming how communications will occur in advance where warranted may avoid confusion and save time over the date change period.

52

## Multilateral Information Sharing

For multilateral information sharing among supervisors, a paradox exists between the need to share information broadly – including sharing some level of sensitive information – and the willingness to share information with supervisors with whom there has been only limited contact or a need-to-know relationship. This paradox may be at least partially overcome by recognising that some Year 2000 issues may have greater regional significance and regional groups may be better positioned to gather and share information, an approach which may be particularly effective for smaller countries and issues that may be regional in nature such as energy, telecommunications, or local settlements<sup>8</sup>. Existing regional groups of supervisors may want to explore this possibility. Such an approach might also be enhanced if larger market supervisors were included in some subset of communications to provide feedback on Year 2000 issues that may be external to the region in order to provide a more global perspective.

Pre-scheduled multilateral calls among public sector participants or public bulletin boards would provide information sharing opportunities primarily for macro level information at the time the rollover occurs or on market conditions during the first business day. These calls are likely to be of the greatest benefit to those that have not yet experienced the particular event.<sup>9</sup> This approach avoids having several hundred individual calls being placed to New Zealand or Australia to see how the date rollover was affecting them. To the extent that the focus of market interest is on infrastructure issues, it may be appropriate to look to the United Nations national coordinators or other public sector bodies rather than having financial regulators look to each other for such information.

In providing information on the macro status of the financial sector or the country more generally, care must be taken to provide information in a timely manner and in a balanced way to avoid over reaction by others having access to the information. This is especially true because some problems will almost certainly occur -- a blanket "everything is fine" statement will often lack credibility if there are even a few known problems in relatively unimportant areas. Similarly, the failure to provide any information may well be interpreted in a way that will magnify any problem and add credibility to any rumours that may develop.

Multilateral calls of an *ad hoc* nature are likely to be required to address Year 2000 issues that have been identified and discussed bilaterally. In many instances, these calls may include selected representatives from both the private and public sector as issues will need to be addressed cooperatively.

---

<sup>8</sup> For example, if telecommunications was experiencing sporadic problems in the Caribbean, individual supervisors in the region might need detailed information on each specific jurisdiction. From the perspective of the London market, however, it might be sufficient to know that there was some level of telecommunications problems in the region and that many organisations were resorting to alternative approaches for processing transactions as developed in their contingency plans.

<sup>9</sup> Note that markets not opening until January 4<sup>th</sup> will be very interested in markets open on January 3<sup>rd</sup> or earlier.

### III. Process Considerations for Implementing Cross-Border Communications

The home/host principles for Year 2000 communications can be applied most effectively if the bilateral parties needing to share information agree in advance on how such communications can best be accomplished. Unlike many home/host communications that occur only after a specific problem is encountered and on an *ad hoc* basis regarding the information to be shared, the date certain nature of Year 2000 provides an opportunity to develop a common understanding on how the communications might unfold.

To this end, bank supervisors will want to identify who the key players are in their market and, for each foreign banking organisation, who the home country supervisor is. Where it is clear that a host country will want to have either *ad hoc* or planned communication with a home country on one or more of the latter's banks, bilateral conversations should take place prior to yearend. Such conversations will help establish both the working relationship necessary for effective communication of sensitive information and specific arrangements for any planned communications.

In some instances, the identification of a single home country supervisor may not be entirely clear.<sup>10</sup> While clarification of specific responsibilities and appropriate channels for sharing general supervisory information is a task beyond the scope of this note, efficient communications on Year 2000 issues require a proactive discussion between home and host supervisors regarding respective roles and communications responsibilities *prior* to the event change period. Where the responsibility is in any doubt, host and home country supervisors should endeavour to identify a single "millennium information coordinator" (MIC) as the contact point to facilitate bilateral communications.<sup>11</sup>

To facilitate the development of home and host country communication protocols, existing regional groups of banking supervisors may want to work together with other Groups like the Basel Committee to develop general procedures for Year 2000 communications during the period. This approach might not only avoid the need for numerous bilateral contacts but also form the basis for scheduled multilateral mechanisms for information sharing.

While this general approach appears widely applicable for sharing Year 2000 information cross-border within the public sector and, in some instances with the private sector, it must be adapted to local market situations. In particular, information needs and flows will likely vary before, during, and immediately after the date rollover depending on local holidays and whether the market is at the leading edge of the rollover or among the last to experience it.

---

<sup>10</sup> For example, in the US, the Federal Reserve would be the home country supervisor for Chase and JP Morgan, the SEC for Goldman Sachs and Morgan Stanley, but there might be some ambiguity for Citigroup because of the OCC's oversight of Citibank, the SEC's oversight of Salomon Smith Barney, and the Federal Reserve's oversight of the overall holding company. Similarly, for a UK subsidiary of a US bank holding company, it is not entirely clear who a third country such as Singapore would view as the home country for a branch of that UK subsidiary.

<sup>11</sup> In instances where there are multiple national supervisors with responsibility for different parts of an organisation and no single umbrella supervisor, MICs might be identified for specific types of information. If an overall picture of the organisation is needed, multiple parties representing the different MICs may need to be present on one side of a bilateral communication. This clearly leads to a level of complexity to the communication and should be avoided if at all possible.