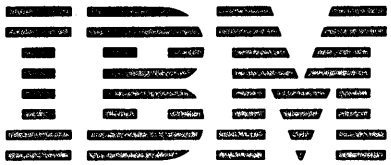


G360-0011-0

INSTALLATION GUIDE

Installation Guide
System/32
System/3

First Edition (April 1977)

A form for readers comments is provided at the back of this publication. If the form has been removed, address your comments to IBM Corporation, Technical Publications, Department 796, P.O. Box 2150, Atlanta, Georgia 30301.

Contents

Introduction

This guide is a planning tool provided to assist you in the successful installation of your IBM system.

One document covers most of the factors that should be considered when planning for the installation of a system. Depending on the nature of your business and the applications being installed, your installation plan may include other factors, while some that are mentioned may not be required.

A computer system is a tool, which to be used effectively, requires effective planning. When all parties concerned understand their respective responsibilities, the installation will be successful and you will more quickly achieve the benefits of using IBM programs and products.

Chapter 1. Responsibilities

As a result of experience gained in the installation of many computer systems, IBM firmly believes that a definition of responsibilities is very beneficial.

IBM

Specifically, it is IBM's responsibility to:

1. Provide the necessary education for your personnel. IBM has provided classes and self-study courses for the executive as well as the installation supervisor, operator and programmer.
2. Provide technical guidance in the use of IBM's systems and applications planning and testing.
3. Provide technical guidance in the physical planning for and installation of your system and IBM applications.
4. Provide customer engineering service for the purpose of maintaining your equipment at a consistently high point of operating efficiency.
5. Keep you advised of new developments in IBM techniques, equipment and applications which apply to your operation.

Note: Some of the above services are on a fee basis.

CUSTOMER

As the customer, it is your responsibility to:

1. Plan an installation schedule which best suits your company's immediate and future needs. This planning document may be used as a guide to develop a specific schedule.
2. Identify the personnel required to staff your installation. It is to your advantage to select persons having a working knowledge or background in the applications that will be a part of your system.
3. Insure that the individuals using the system utilize the available self-study and classroom education, understand the capabilities of the system, know how to install it and how to use it effectively.
4. Convert your existing files into the files that will be used for your applications. You must also provide adequate protection from accidental loss or misuse of data.
5. Review with the IBM Representative, your business volumes including present and future needs, so that you can plan for the proper system configuration.

6. Insure that the required hardware and program prerequisites are available for implementation and execution of any proposed application.

Many of these responsibilities are dependent upon one another; therefore, it is important that both parties satisfy their obligations. IBM also recognizes that emergencies or critical situations may develop which might require exceptions.

These responsibilities are outlined here to provide a logical approach to a successful installation program. The foundation of this program is the fact that your company and IBM are dedicated to the establishment of a data processing installation which is mutually productive and profitable.

System Description and IBM Support

This section identifies the specific IBM equipment you have ordered, the applications which you expect to process on the equipment, the specific individuals within IBM who will be involved in your installation, and the IBM support manuals that you should have as part of the working documentation.

A. Equipment Ordered

Machine Description	Machine Type	Machine Model	Monthly Availability Charge	Term Lease Price	Purchase Price	Scheduled Shipment Date

B. Applications to be Processed

Application Name	Number of Master Records	Monthly Transaction Volume	Target Conversion Date

C. IBM Support Team

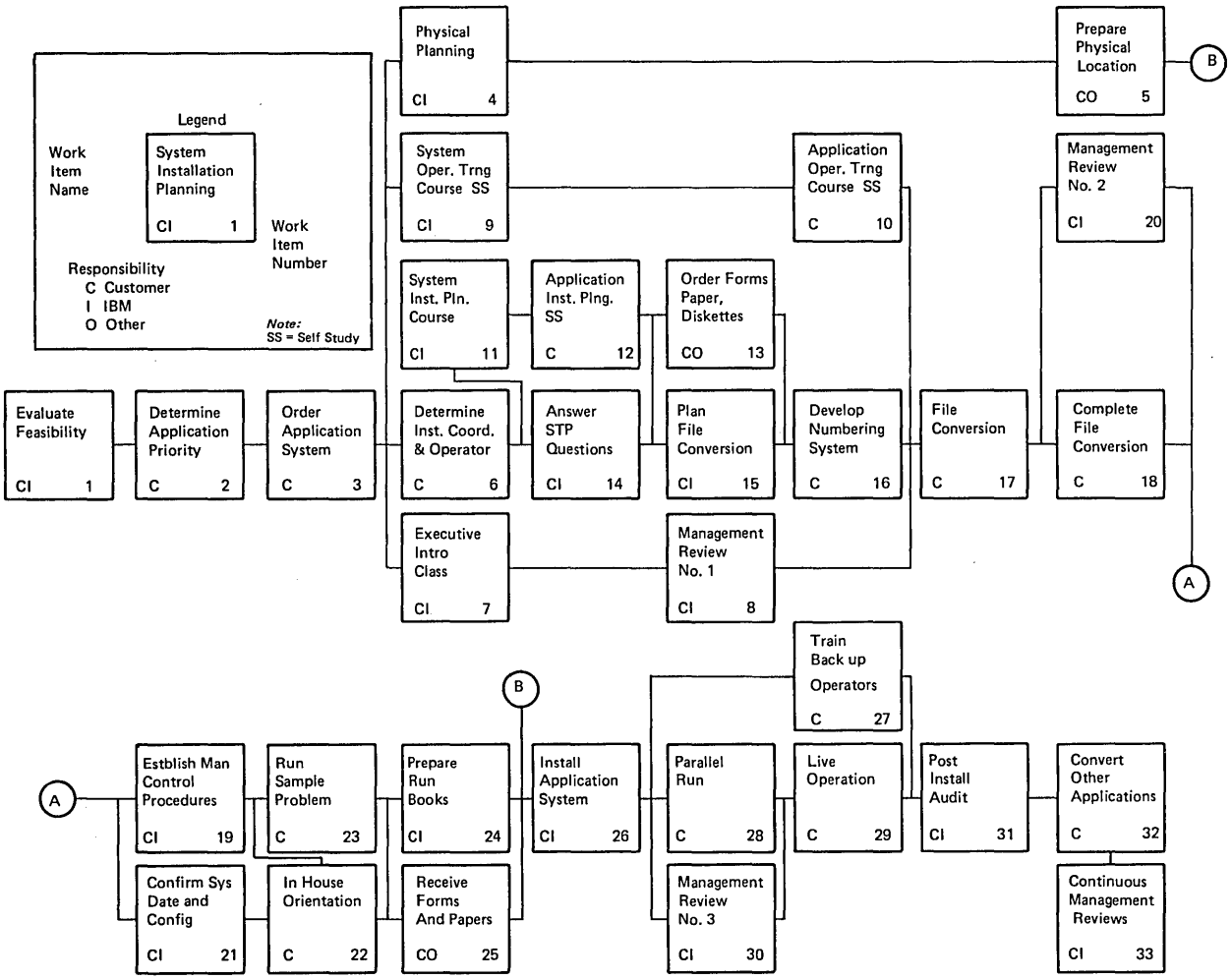
Initial contact between you and these individuals will be organized through your IBM Sales Representative.

Name	Title	Telephone Number
	Sales Representative	
	Systems Engineer	
	Customer Engineer	
	Programming Support Representative	
	Marketing Manager	

Name	Title	Telephone Number
	Systems Engineering Manager	
	Customer Engineering Manager	

Chapter 2. Installation Plan

This section identifies the major events which should occur in the course of a successful system installation program.



Target dates for the various events should be established and shown on the Installation Planning Schedule, Figure 2.2.

For: _____

Installation Date: _____

No.	ACTIVITY	RESPONSIBILITY	WEEKS 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	SYS Delivery 1 2 3 4 5 6 7 8 9 10
1.	Evaluate Feasibility	C-I		
2.	Determine Application Priorities	C		
3.	Order System	C		
4.	Physical Site Planning	C-I		
5.	Prepare Physical Location	C-O		
6.	Determine Inst. Coord. and Operator	C		
7.	Executive Introduction Class	C-I		
8.	Management Review No. 1	C-I		
9.	Operator Training Class	C-I		
10.	Application Operator Training Self Study	C		
11.	Installation Planning Class	C-I		
12.	Application Installation Planning Self Study	C		
13.	Order Forms, Paper, Diskettes	C-O		
14.	Answer STP Questions	C-I		
15.	Plan File Conversion	C-I		
16.	Develop Numbering System	C		
17.	File Conversion	C		
18.	Complete File Conversion	C		
19.	Establish Manual Control Procedures	C-I		
20.	Management Review No. 2	C		
21.	Confirm System Configuration & Date	C-I		
22.	In-House Orientation	C		
23.	Run Sample Problem	C		
24.	Prepare Run Books	C-I		
25.	Receive Forms and Paper	C-O		
26.	Install Application System	C-I		
27.	Train Back-Up Operator	C		
28.	Parallel Run	C		
29.	Live Operation	C		
30.	Management Review No. 3	C-I		
31.	Post Installation Audit	C-I		
32.	Convert Other Applications	C		
33.	Continuous Management Reviews	C		

Figure 2.2. Installation Schedule

While there are 26 weeks shown on the schedule, actual installation time will vary, depending on the complexity of the applications to be installed. Use only that portion of the plan which is applicable to your installation.

System installation can be broken into three phases:

1. Pre Installation
2. Installation
3. Post Installation

The responsibility of the activities in the three phases has been mentioned in the Responsibility Section of this document.

The activities included in each phase are:

1. Pre Installation
    a. Personnel Selection
    b. Physical Planning
    c. Education
    d. User Department Training
    e. Data Gathering
    f. File Conversion
    g. Testing of Data in Files

2. Installation

    a. System Installation
    b. Application Installation

3. Post Installation

    a. Education
    b. Creation of Master Files
    c. System Conversion
    d. Backup
    e. Installation of Additional Applications

INSTALLATION PROGRESS MEASUREMENT TECHNIQUE

Advantages for the Executive

- Receives reasonable, periodic checkpoints on the progress of the DP staff.
- Progress reviews consume a minimum of everyone's valuable time.
- DP staff requirements are clearly visible at all times.
- Sees continuing evidence of IBM interest and support.
- Necessary changes in talent or facilities can be recognized early.
- Installation costs are minimized.

How It Helps the DP Manager

- Weighted goals are easier to understand.
- Requests for additional resources are more solidly based.
- More time is available to *make* progress—less time is consumed in *reviewing* progress.

How It's Done—the Technique

First, establish point values. List all programs to be completed at the time of installation. Assign each a relative weighted value from one to nine, based on the degree of difficulty anticipated.

Then divide the sum of all weighted points by the number of weeks planned for defining, coding, testing, and documenting these programs. The resulting number sets the number of points that must be earned each week to stay on schedule.

Earning the Points

Points are earned according to the percentage of completion attained for each program based on the relative weight of each program. The percentages are set up as follows:

Program	Percentage
Defined	10%
Coded and keypunched/recorded	40%
First compile or first test	10%
Tested and documented	40%

Points are earned and recorded weekly for each program, using the percentages above, and are then summarized to show the following highlights:

- Weeks remaining until installation time
- Points earned during current week
- Points earned to date
- Points needed to date
- Points *ahead* of schedule
- Points *behind* schedule

Initial Documentation—Installation Planning Schedule

If you have never used an Installation Planning Schedule, try it. You'll find it very helpful. Form GX20-8010 is designed for manual entry. Form GX60-0034 is designed for typewriter entry.

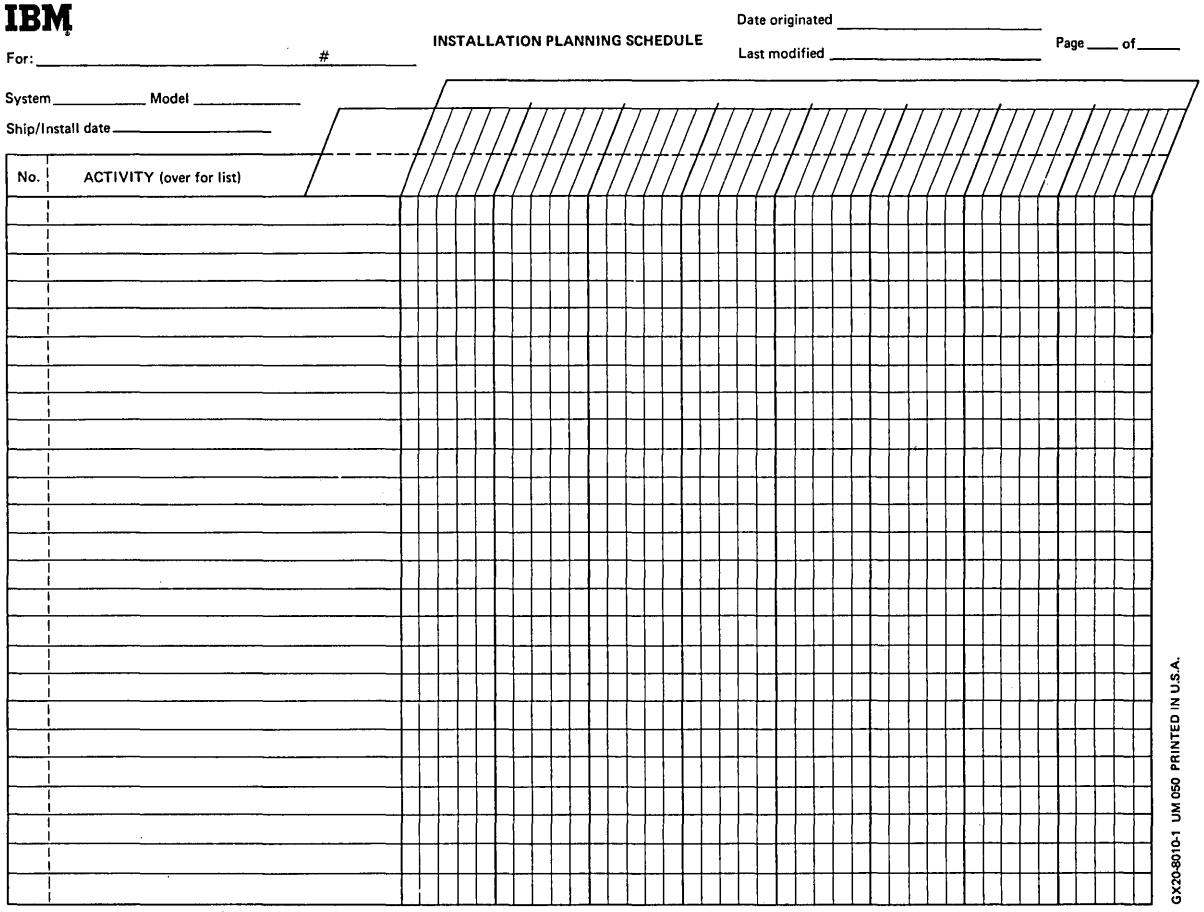


Figure 2.3A. Installation Planning Schedule (GX20-8010)

TYPES OF ACTIVITIES INVOLVED IN ESTABLISHING AN INSTALLATION PLANNING SCHEDULE

Order System, Support Services, Disk Packs, Data Cartridges
Give Aptitude Tests
Select staff
Education (list each course)
Document current procedures
General Systems Design (workflow)
Physical Site Planning
(Customer Engineering check if hazardous/ contaminated environment is suspected)
Common Carrier arrangements
Mgmt. Progress Reviews (recurring)
Select Program Products
Select Field Developed Programs
Select Industry Application Programs (IAP)
Detail Systems Design
Order Field Developed Programs
Order System disk pack, Data Cartridge
Preliminary File Conversion plans
Application Program Development
(allow for coding, testing, debugging, and documentation)
Confirm System delivery
Order forms, supplies & accessories
Order Program Products
Order IAPs

Finalize File Conversion plans
Operator training (may have before and/or after installation)
Run Books Documentation
(operating procedures)
Customer Engineering Review of Physical Site
In-house Education
(orientation of other personnel who may be affected by input requirements & output)
Install data recorder or 3741
(for early file conversion if planned)
Disk pack delivery/ Data Cartridge delivery
File Conversion – (application)
System Test (complete processing cycle)
(before installation if possible)
Install System
(Additional) Operator Training

File Conversion (if not used earlier) } repeat for
Parallel or Pilot operation } each
Cut-over } application

System Evaluation

The listing above is not meant to be exhaustive. Systems that involve sensor based and Communications applications will have additional associated activities that should be included in the installation plan

Figure 2.3B. Installation Planning Activities

This is a sample of the activities involved in installing the system—from the point of ordering—up to installation. Your plan can include other activities that may occur before and after these times.

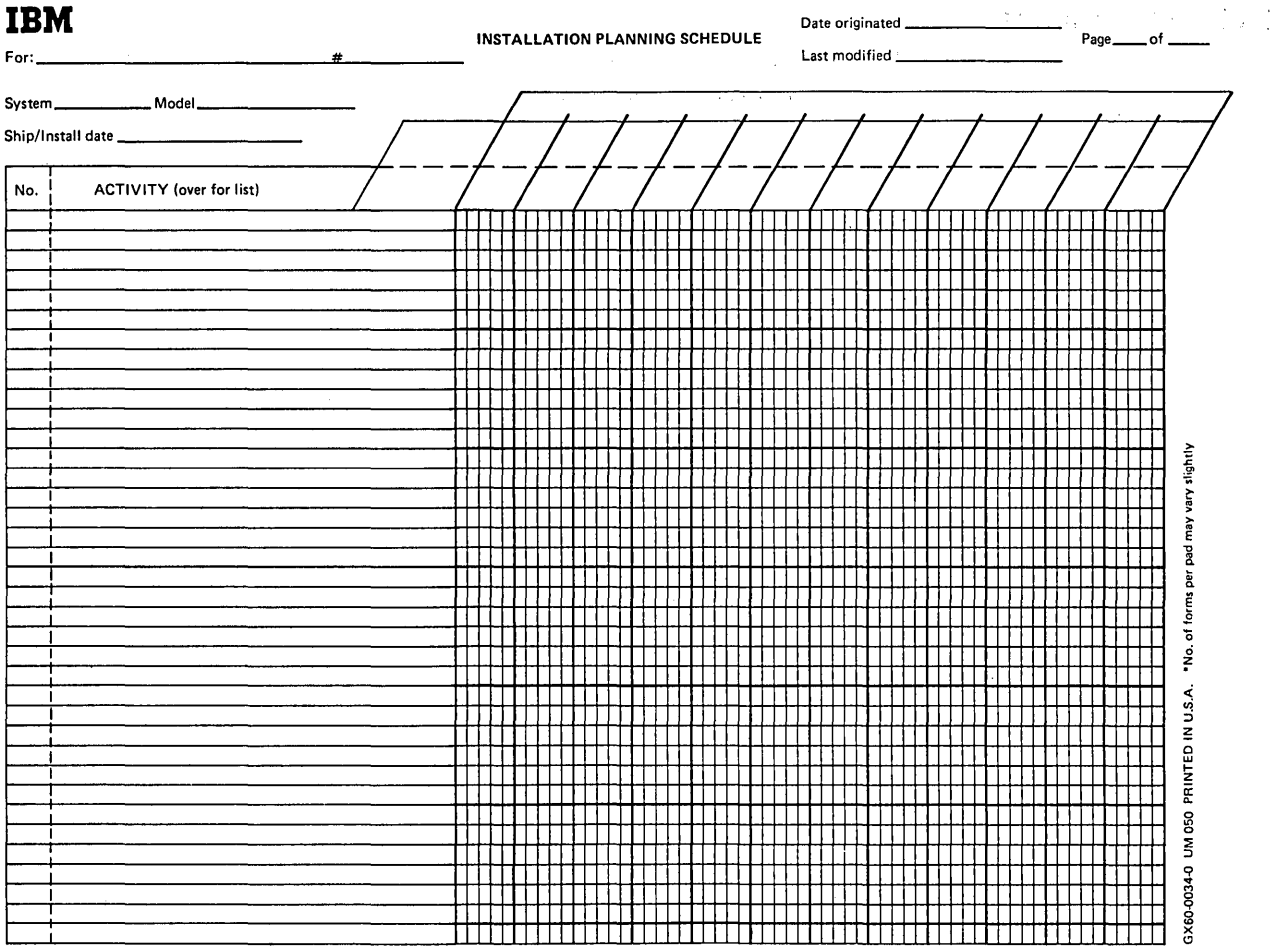


Figure 2.3C. Installation Planning Schedule (GX60-0034)

List the activities in the order that best fits your situation. Double spacing of the activities is recommended for easy reading. List your activities in the order that makes it easy to understand. The exact order need not be rigid because some activities will overlap anyway.

In the column that identifies the current week list the date during the week on which that activity first occurs. Alongside that date you may want to show how many days this acitivity will take. You may want to use a dash to separate the date and the number of days. If the activity is expected to take several weeks, you may want to draw a bar to represent that time period.

Please note that executive agreement to the installation plan is prerequisite to further development.

General Systems Design

Chart each application on a separate worksheet. Either side of the Diagramming and Charting Worksheet, Figure 2.4A or 2.4B, (GX20-8021) is suitable for this purpose.

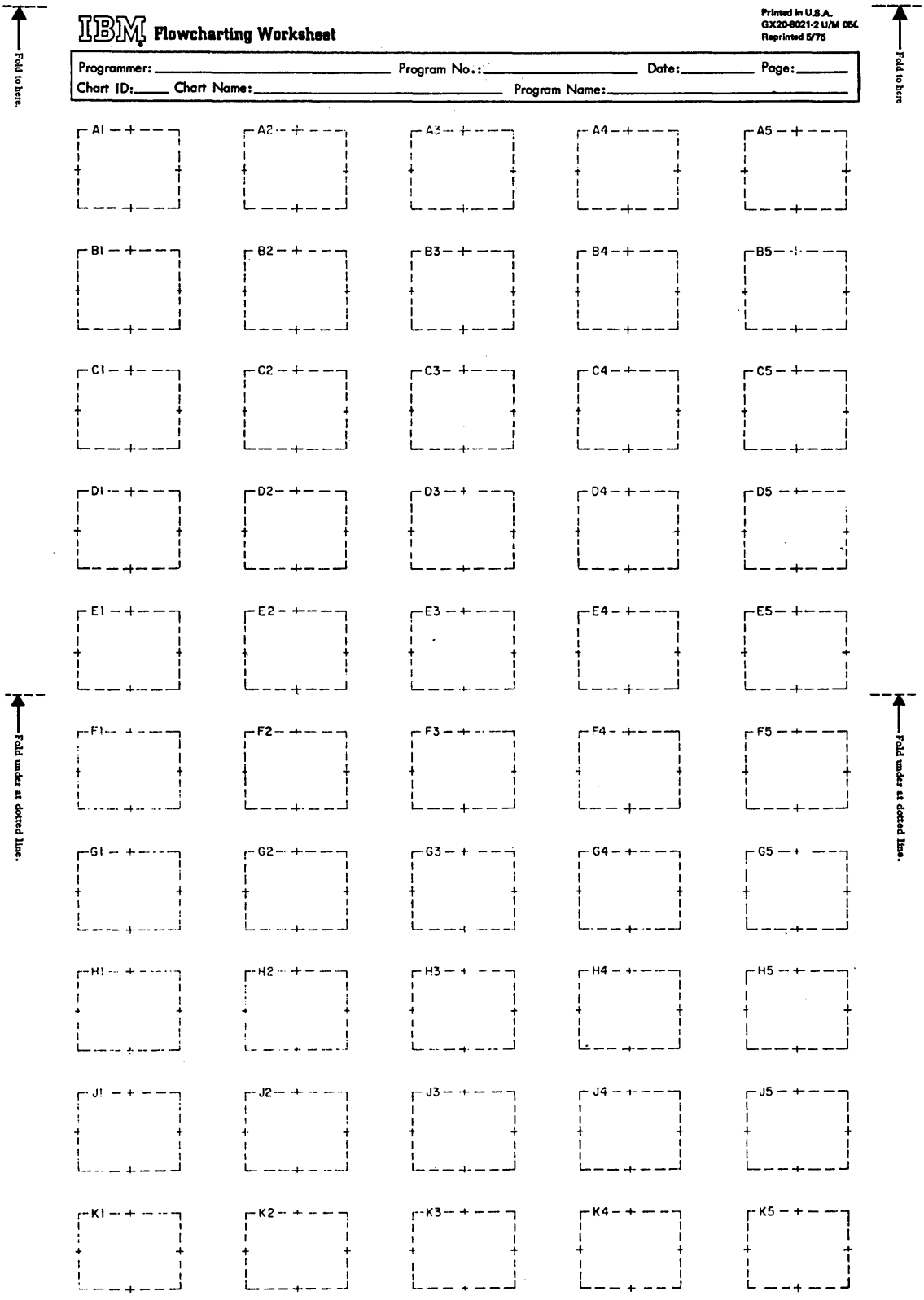


Figure 2.4A. Charting Worksheet (GX20-8021)

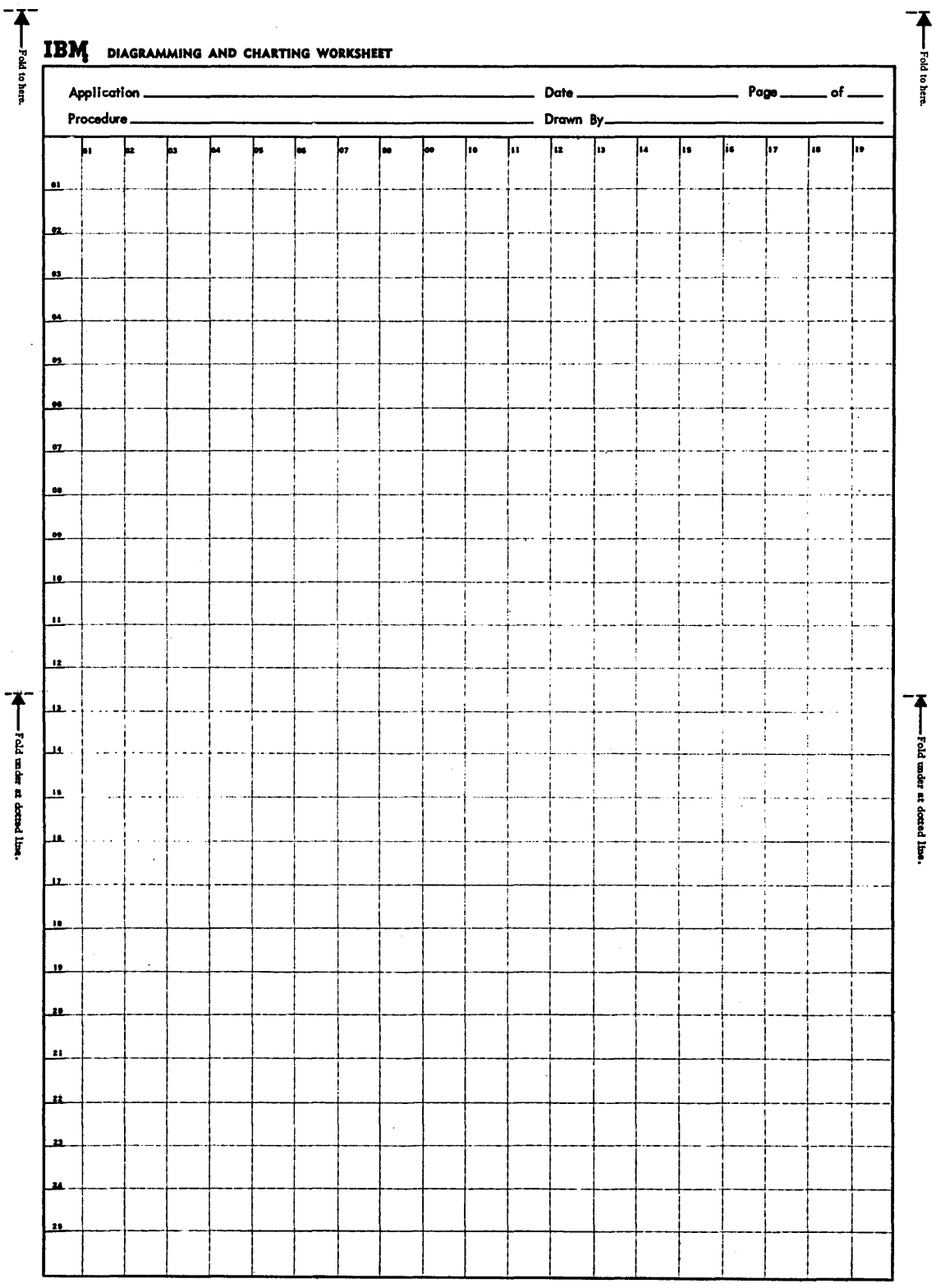


Figure 2.4B. Charting Worksheet

Use the Flowcharting Template (GX20-8020) with this worksheet.

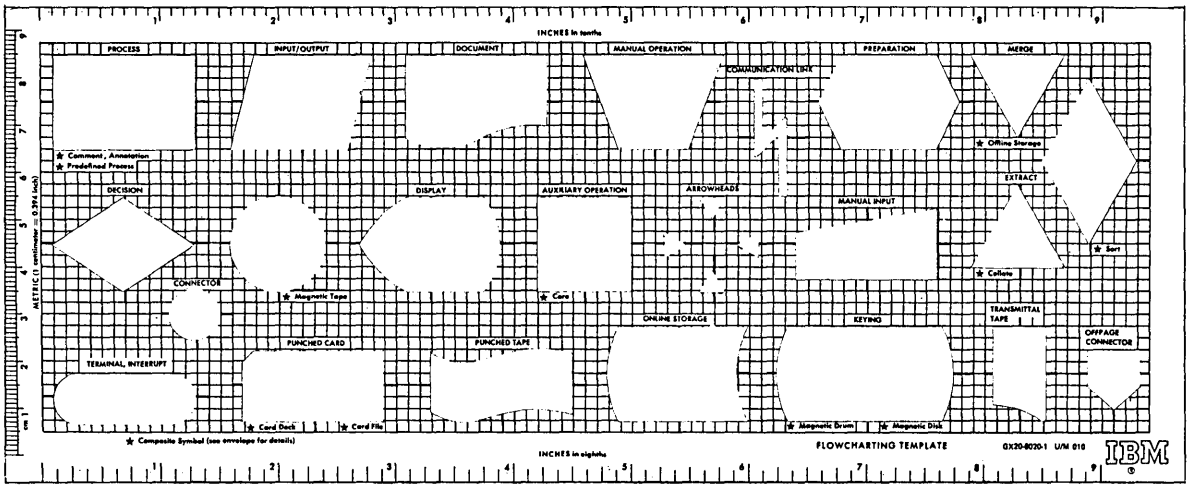


Figure 2.5. Flowcharting Template (GX20-8020)

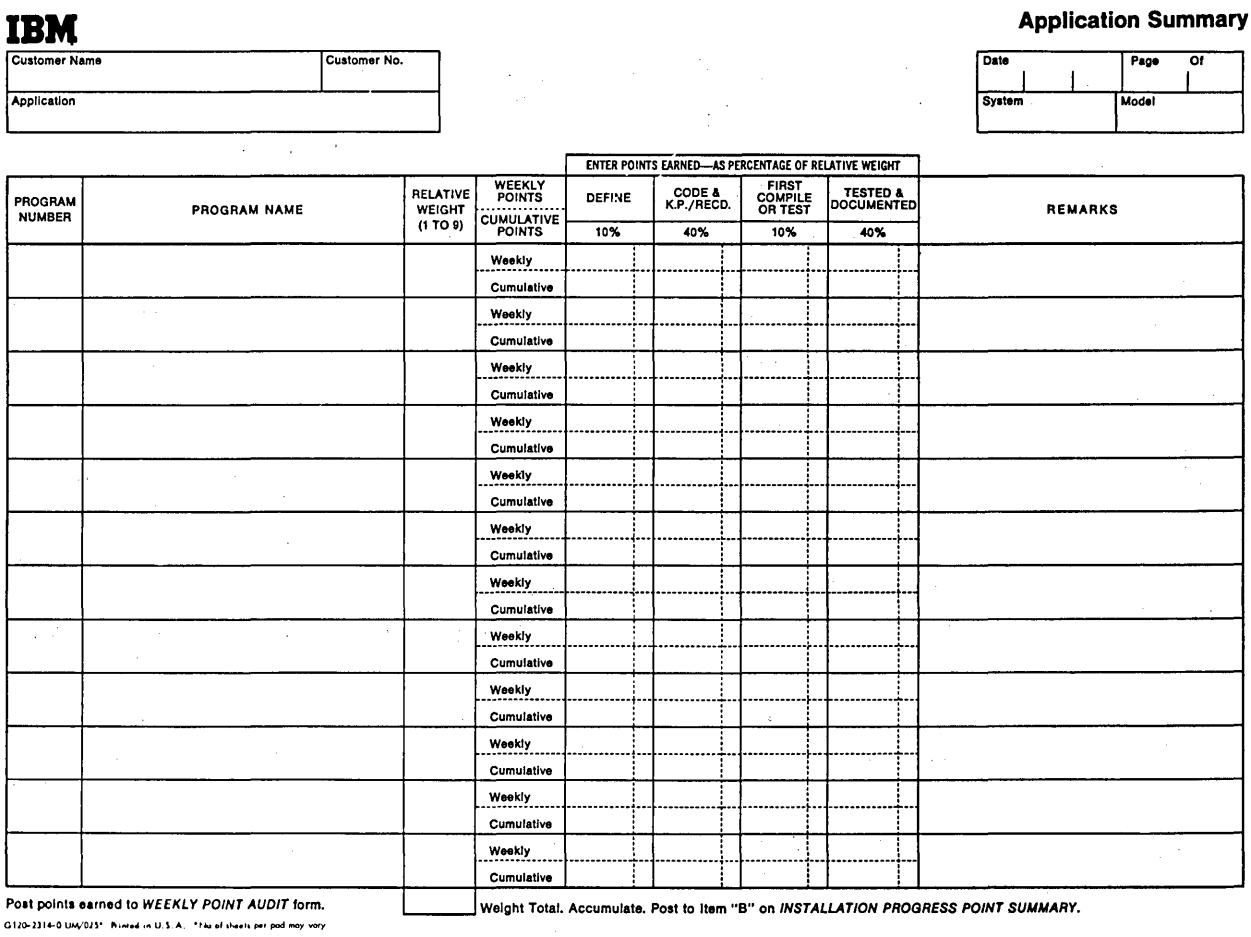
The chart should depict the general flow of work in the system, as planned for at the time.

Identify each program involved in the application on the chart by name and/or number. Leave number gaps for programs added later. Include utility programs as well.

Develop the general systems design with the assistance of the DP manager and a systems engineer.

Application Summary

Begin each application on a separate sheet (Form G120-2314).



IBM **Application Summary**

Customer Name	Customer No.	Date	Page Of
Application		System	Model

				ENTER POINTS EARNED—AS PERCENTAGE OF RELATIVE WEIGHT				
PROGRAM NUMBER	PROGRAM NAME	RELATIVE WEIGHT (1 TO 9)	WEEKLY POINTS CUMULATIVE POINTS	DEFINE	CODE & K.P./RECD.	FIRST COMPILE OR TEST	TESTED & DOCUMENTED	REMARKS
				10%	40%	10%	40%	
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
Post points earned to *WEEKLY POINT AUDIT* form.			Weight Total. Accumulate. Post to Item "B" on *INSTALLATION PROGRESS POINT SUMMARY.*					

G120-2314-0 UM/025* Printed in U.S.A. *No. of sheets per pad may vary

Figure 2.6. Application Summary (G120-2314)

List on the Application Summary form each program, identified in the general systems design, to be written or modified for this installation prior to install time. Do this whether the work is to be done by your staff alone, or with IBM assistance.

Assign a relative weight ranging from one to nine to each program listed. This weight should reflect the degree of difficulty anticipated in defining, coding, testing, and documenting each program, or modifying a program supplied by IBM.

Assign the highest weight of nine to the most difficult program to be completed prior to installation, taking into consideration all applications involved. All other programs should receive weights relative to the most difficult one. More than one program may be assigned the highest weight.

A simple utility could be assigned the weight of one, while "invoicing" could be assigned a weight of nine. Extensive experience with this technique has shown that "forcing" an average weight near five helps avoid grossly *over-* or *under*-weighting the programs.

It is not necessary to spend a lot of time deciding on accurate weights. The object is to set some goals, and then work toward those goals.

Leaving Yourself an Opening

List one or more "open" programs, which may be 10 to 20% of all programs, for each application, if it is probable that additional programs will be needed—even though not as yet identified. This provides a buffer to soften the effect of undue optimism or disappointing talents.

Accumulate the weight totals by application. Post the overall total to the upper right side of the Installation Progress Point Summary form, as will be explained under "Measuring Progress."

Weekly Point Audit

Don't use the form (G120-2316) until the end of the first week in which you begin earning points (first week of Detail Systems Design on the Installation Planning Schedule).

Use form shown in Figure 2.7 during every update session until installation to tally the points earned since the last update session. This will be explained further under "Measuring Progress."

IBM **Weekly Point Audit**

Customer Name*	Customer No.	System	Model	Page	Of

APPLICATION AND PROGRAM NUMBER	ENTER "AS OF" DATES																	
	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/

Z120-2315-0 (U/M 025)

Accumulate weekly points earned. Post to *INSTALLATION PROGRESS POINT SUMMARY* form.

Figure 2.7. Weekly Point Audit (G120-2315)

Installation Progress Point Summary

Fill out the upper part of this form (G120-2316) after the Application Summary forms are completed for all applications.

IBM **Installation Progress Point Summary**

Customer Name		Customer No.
System	Model	Ship/Install Date

A. Number of weeks in Plan (to define, code, test and document) .....

B. Weight totals (total points from Application Summaries, needed prior to Install) .....

C. Average points/week needed (for on-time Install) (B ÷ A) .....

First "Weeks Remaining" column used should coincide with the first week of "Detail Systems Design" on Installation Planning Schedule.

"As of" Dates	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Weeks Remaining	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
Points Earned This Week															
Points Earned To Date															
Points Needed To Date															
Ahead of Schedule (+)															
Behind Schedule (–)															

(continued)

"As of" Dates	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Weeks Remaining	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Points Earned This Week																INSTALLATION / CONVERSION
Points Earned To Date																
Points Needed To Date																
Ahead of Schedule (+)																
Behind Schedule (–)																

G120-2316-1 (U/M 025)

Figure 2.8A. Installation Progress Point Summary (G120-2316)

Item A should be determined from the Installation Planning Schedule. "A" is the number of weeks in the plan, starting with the first week of the detailed systems design, and includes all the weeks planned for defining, coding, testing, and documenting the programs to be completed prior to system installation.

Item B is arrived at by adding all the relative weight points for all the programs which are defined on the Application Summary forms.

Item C is calculated by dividing B by A, to arrive at the average number of points needed per week to stay on schedule and install on time.

When C is known, fill in the "Points Needed To-Date" lines, starting with the appropriate "Week Remaining" column. Cross out the columns to the left of the first one used.

The first entry in "Points Needed To-Date" should be the value of C, the next entry "two times C", the next entry "three times C", etc. The final entry under "Weeks Remaining—1" should equal B in the upper part of the form.

If C is not a whole number, the final "Points Needed To-Date" number may show a fractional difference from B. It should not be significant. If it is, recheck the figures for accuracy.

Enter the "As Of" dates (last date in the week) above "Weeks Remaining" starting with the week corresponding to the first week of Detail Systems Design on the Installation Planning Schedule.

Make no entries in the other fields until the end of the first week in the Detail Systems Design, or immediately following that week.

After completing the initial documentation, cover the plan with the executive for his concurrence. Then explain it to the DP manager.

Getting Earned Points Down on Paper

Record points earned in weekly increments, even if not reviewed that often. If you are not at least *two weeks* ahead of schedule, it may be best to review weekly in order to keep on top of the situation.

Measuring Progress

First, look at the Application Summary form. A percentage of the relative weight assigned to each program is earned as definition, coding, compilation/testing, and documentation are completed.

For example, a program which has a relative weight of seven would receive an earned value of 0.7 after being defined, and 2.8 after being coded and keypunched. The cumulative points earned up to this time total 3.5.

After the program has been compiled or tested for the first time, an additional 0.7 points is earned (cumulative 4.2).

After testing and documentation of that program is complete, an additional 2.8 points bring the total up to 7.0 for that completed program.

Holding out this big percentage earning for testing and documenting is very important in motivating your people to get each program completed and "on the shelf", ready for use. A poorly documented program, even though debugged, can present major problems later on. Documentation should include an operator's console run book.

During weekly recording, or when the "Earned Percentage" is entered on the Application Summary form for each program, immediately record points earned on the Weekly Point Audit form. If all the Application Summary forms were updated first and then posted to the audit form, some earnings might be incorrectly transcribed since the summary form for applications does not have a weekly breakdown.

The Application Summary will show the current status of each program, whereas the Weekly Point Audit is simply a worksheet for accumulating earned points.

After you have updated all applications, post the total points earned for the week, as indicated on the Weekly Point Audit form, to the Installation Progress Point Summary.

Eventually, the Application Summary begins to look like a detailed "GANTT" chart.

The cumulative points earned for each program, as shown on the Application Summaries, can be easily added and balanced to the "Points Earned To-Date" field on the Installation Progress Point Summary when it is updated for the week, if a cross-check is needed.

After you have posted the "Points Earned This Week" to the Installation Point Summary form, the cumulative "Points Earned To-Date" field can be updated.

Compare the points earned to "Points Needed To-Date", and enter the difference as appropriate in the "Ahead of Schedule" or "Behind Schedule" field. *This is the key entry.* It may be used during your regular Progress Review with the DP manager and the executive to determine the following:

- Number of weeks ahead of or behind schedule (latest entry divided by C)
- Whether additional resources are needed
- Whether additional training is needed
- Whether the system ship schedule should be deferred or improved

Also, if a definite downward trend in an "Ahead of Schedule" situation is detected, this trend should be mentally extended in planning to see if the schedule can, in fact, be met if the trend continues.

The reverse side of this form (Figure 2.8B) provides a convenient area for keeping a running summary of fee services expenditures.

SYSTEMS ENGINEERING SERVICES

DATE	EXPENDED	BUDGETED

EDUCATION

DATE		CLASS No.	EXPENDED	BUDGETED
SCHEDULED	COMPLETED			

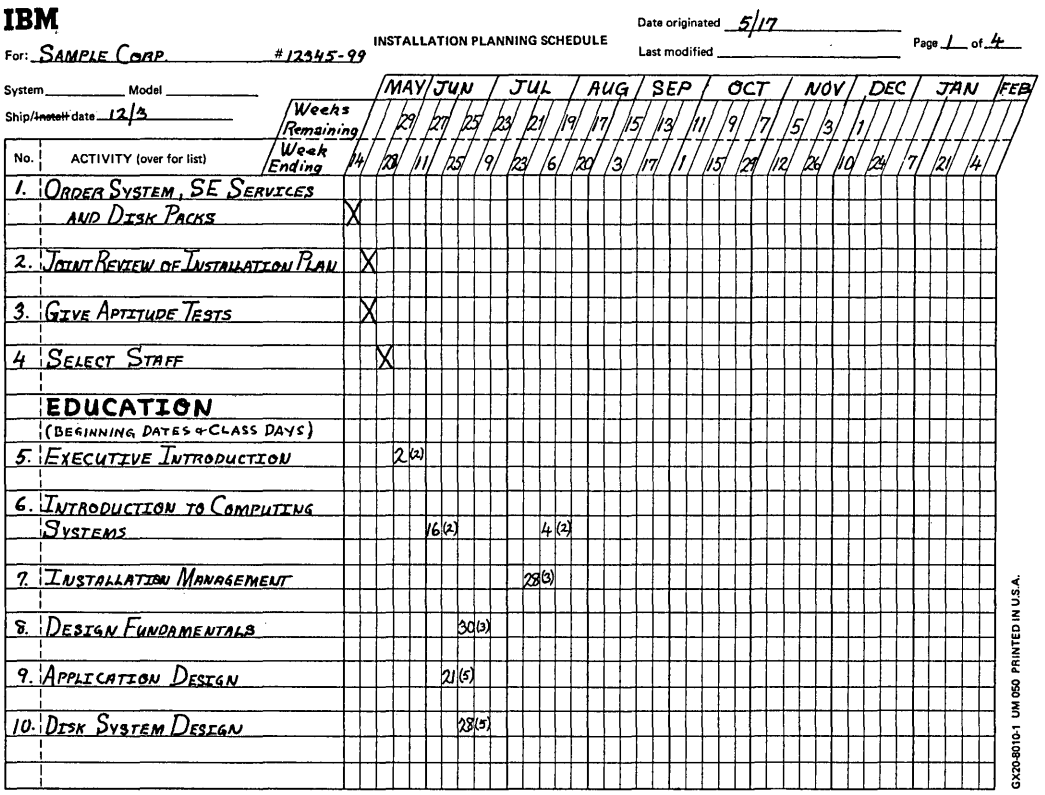
Figure 2.8B. Services Log (G120-2316)

Example

Consider the following example for a clearer understanding of how the forms are used. The example involves systems design and program development.

You ordered a system during the week ending May 14. You drew up an Installation Planning Schedule (Figure 2.9) based on a mid-December installation date. In this case, because executive agreement to the plan had not been obtained as yet, joint review of the plan by your management and the IBM representative was included as the *very next* item of business. Getting total agreement to the plan is one of the keys to success.

The four pages in this plan depict most of the activities and relative time frames to be agreed upon for the system/model involved. Specific cases may vary. Other types of systems may involve a different mixture of activities.



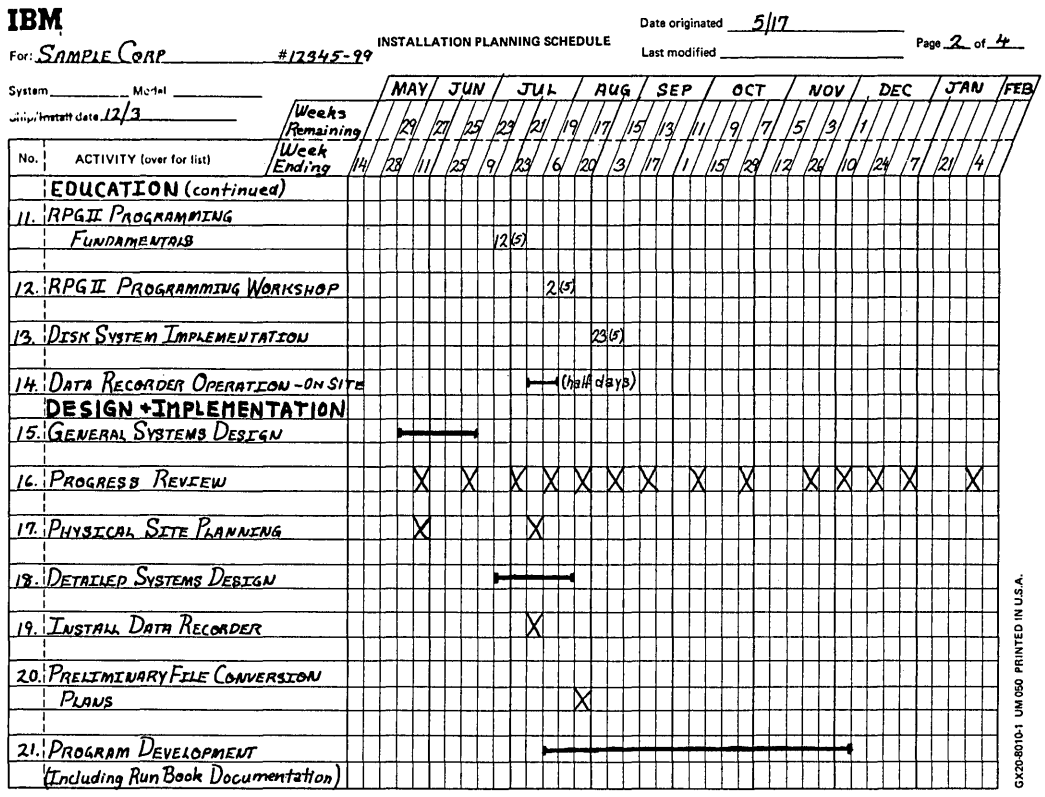
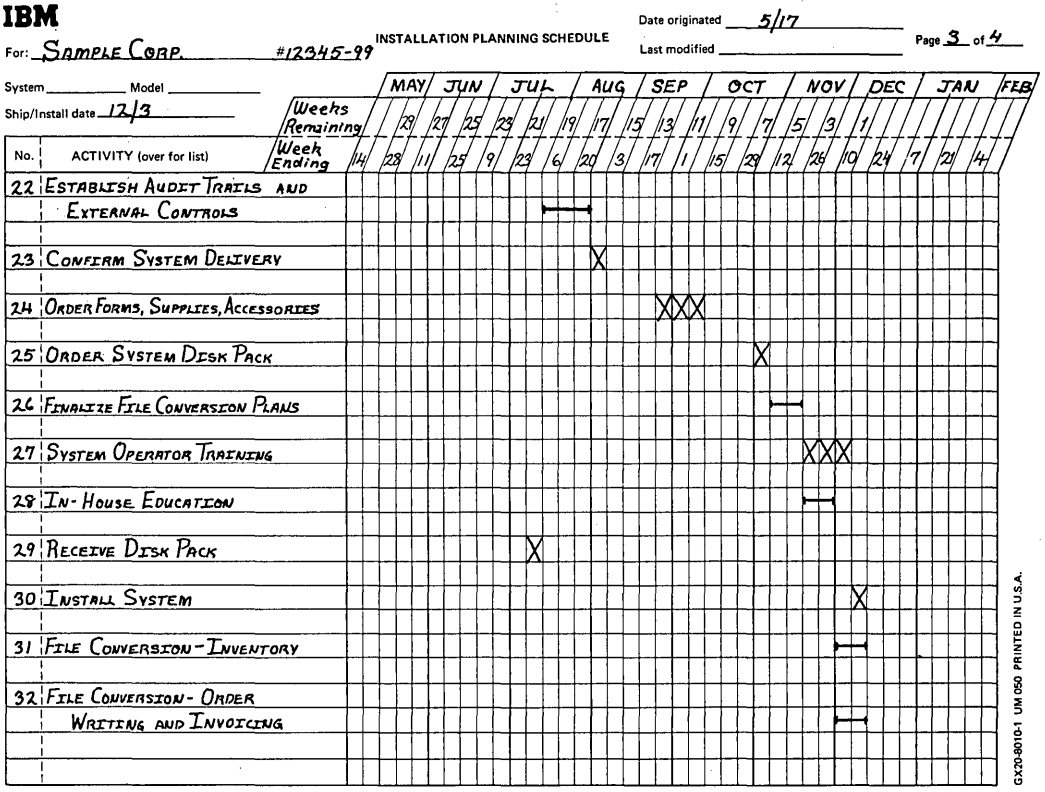


Figure 2.9A. Example Installation Planning Schedule



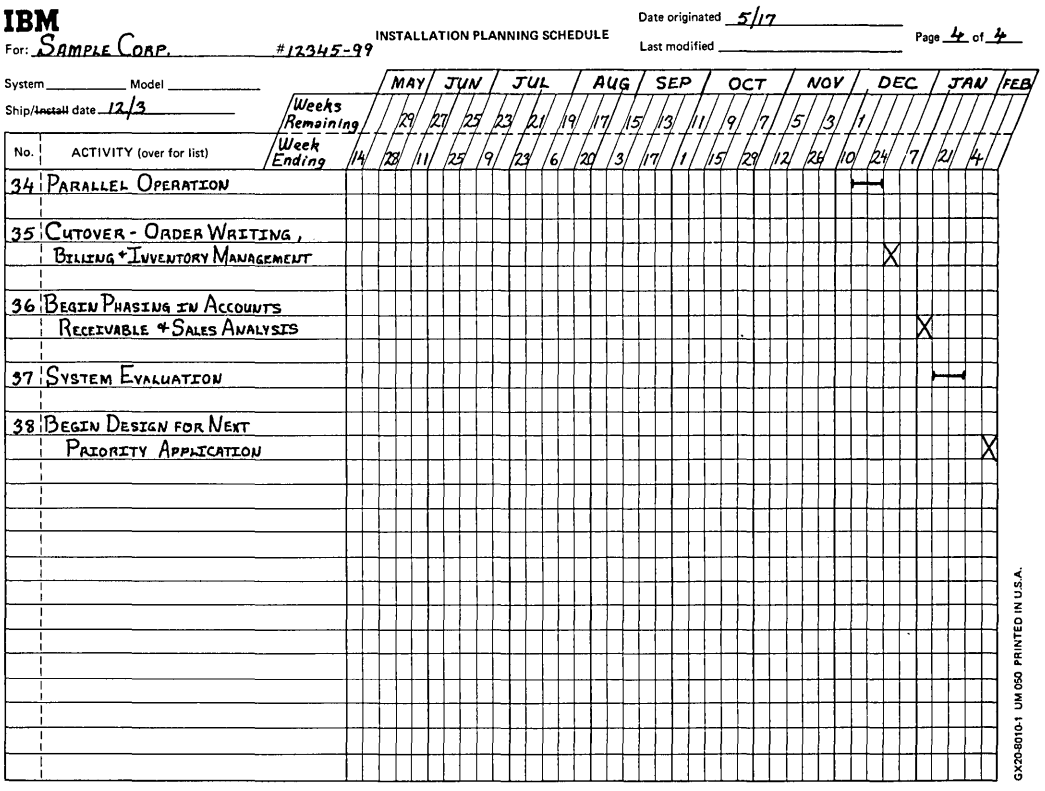


Figure 2.9B. Example Installation Planning Schedule

Most of the heading area on this form is self-explanatory. Either the ship or install date may be shown. Delete the word that does not apply. The vertical columns for weeks may be used as desired; i.e., each group of five columns can be used for a month, or the heavy lines can be ignored and all columns can be used for weeks running continuously. The latter method was used for this example. In this way, bar graphs clearly indicate the number of weeks planned for an activity. For added convenience, names of months can be written in the uppermost horizontal part of the columns.

The slanted area can be used as shown, with the lower half indicating "week ending" dates of future weeks and the upper half indicating the number of "weeks remaining" prior to installation time. Only every other column is identified to make the dates and numbers easier to read.

The example may not fit your needs exactly. It simply establishes some time frames to show how weighted values are established and how points are earned using this technique.

Look at item 15 (General Systems Design). At this point, the general flow of work through the data processing system must be charted. Refer to Figure 2.10.

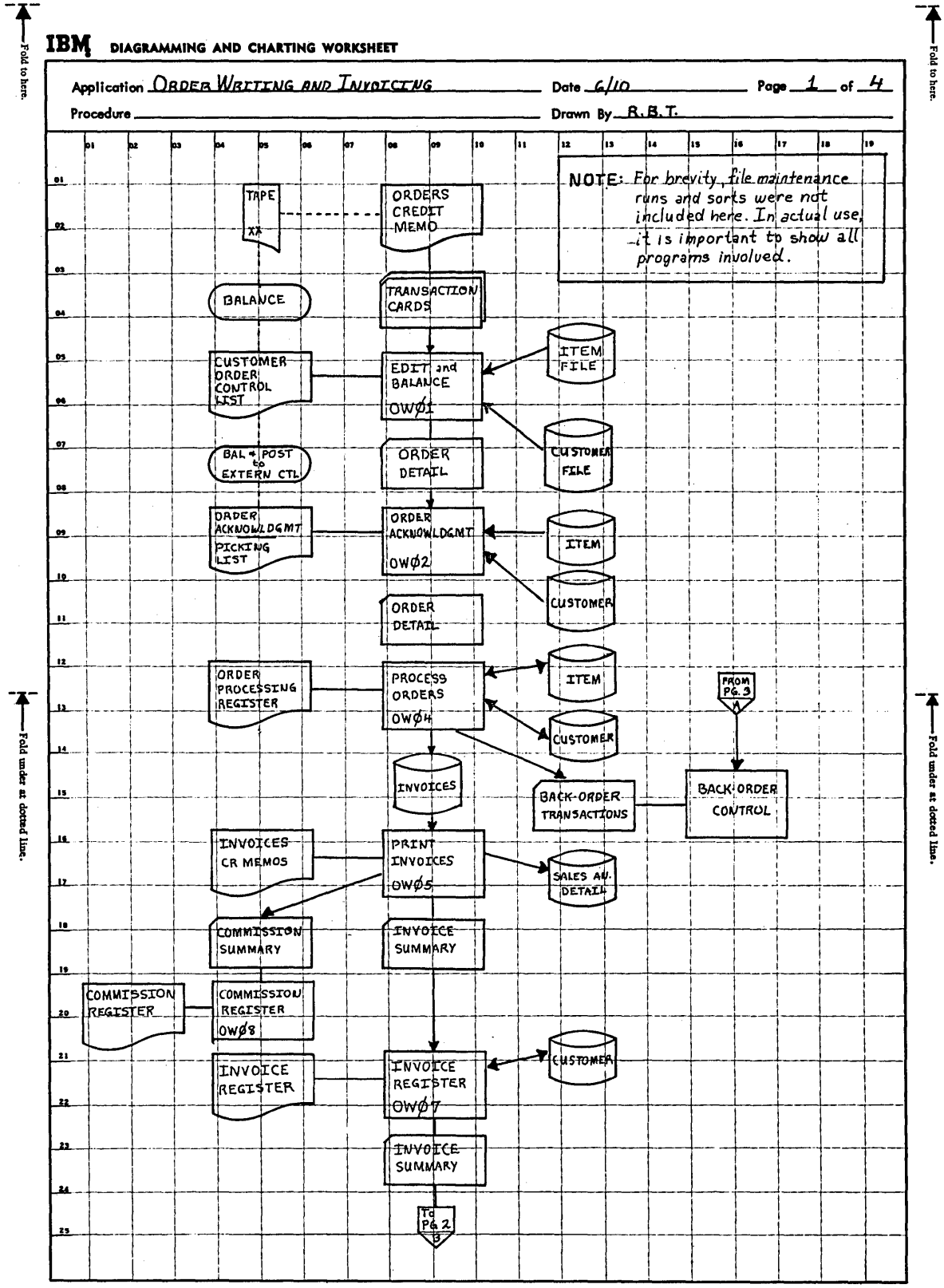


Figure 2.10A. Example General System Design—Order Writing and Invoicing

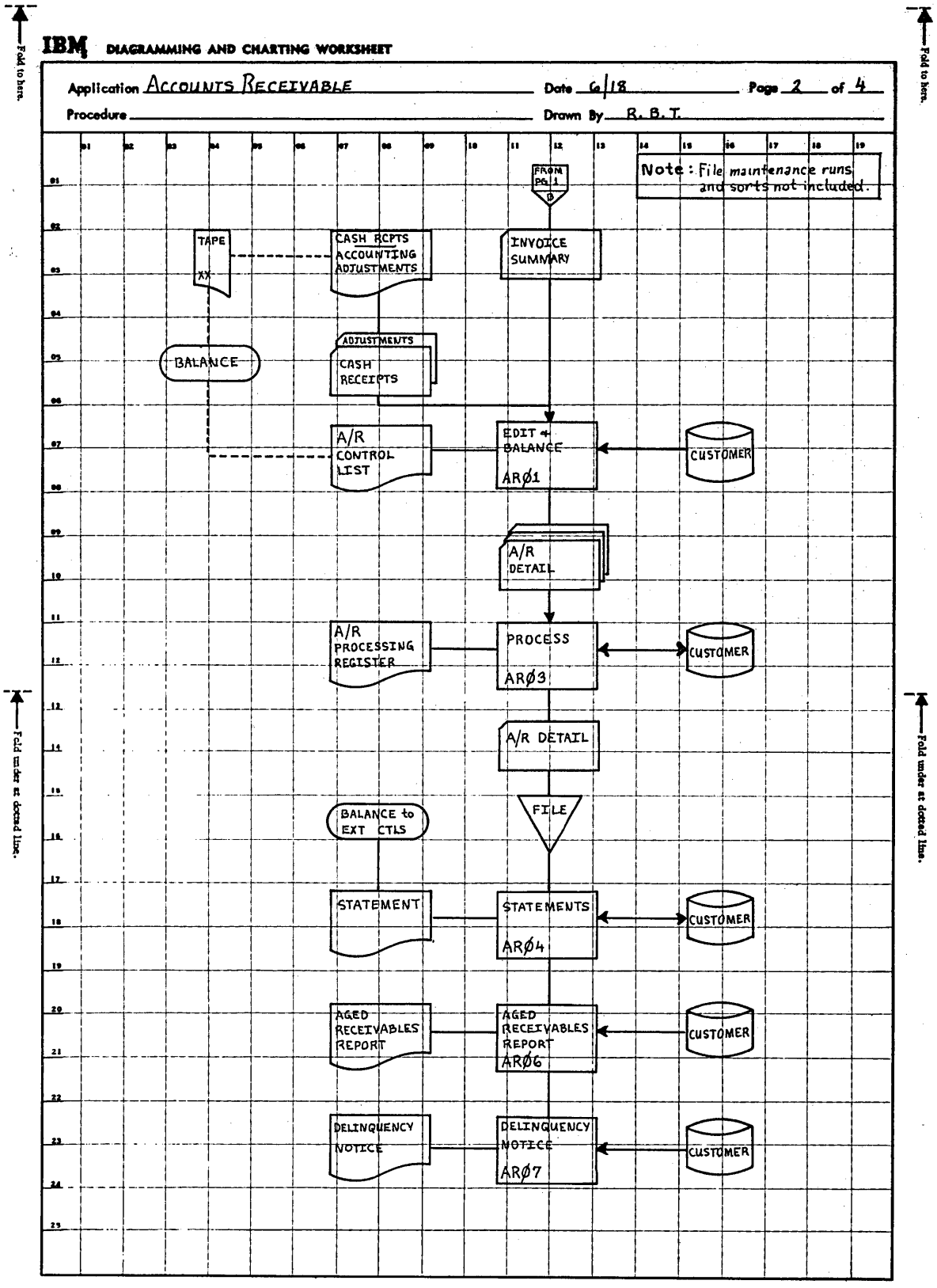


Figure 2.10B. Example General System Design—Accounts Receivable

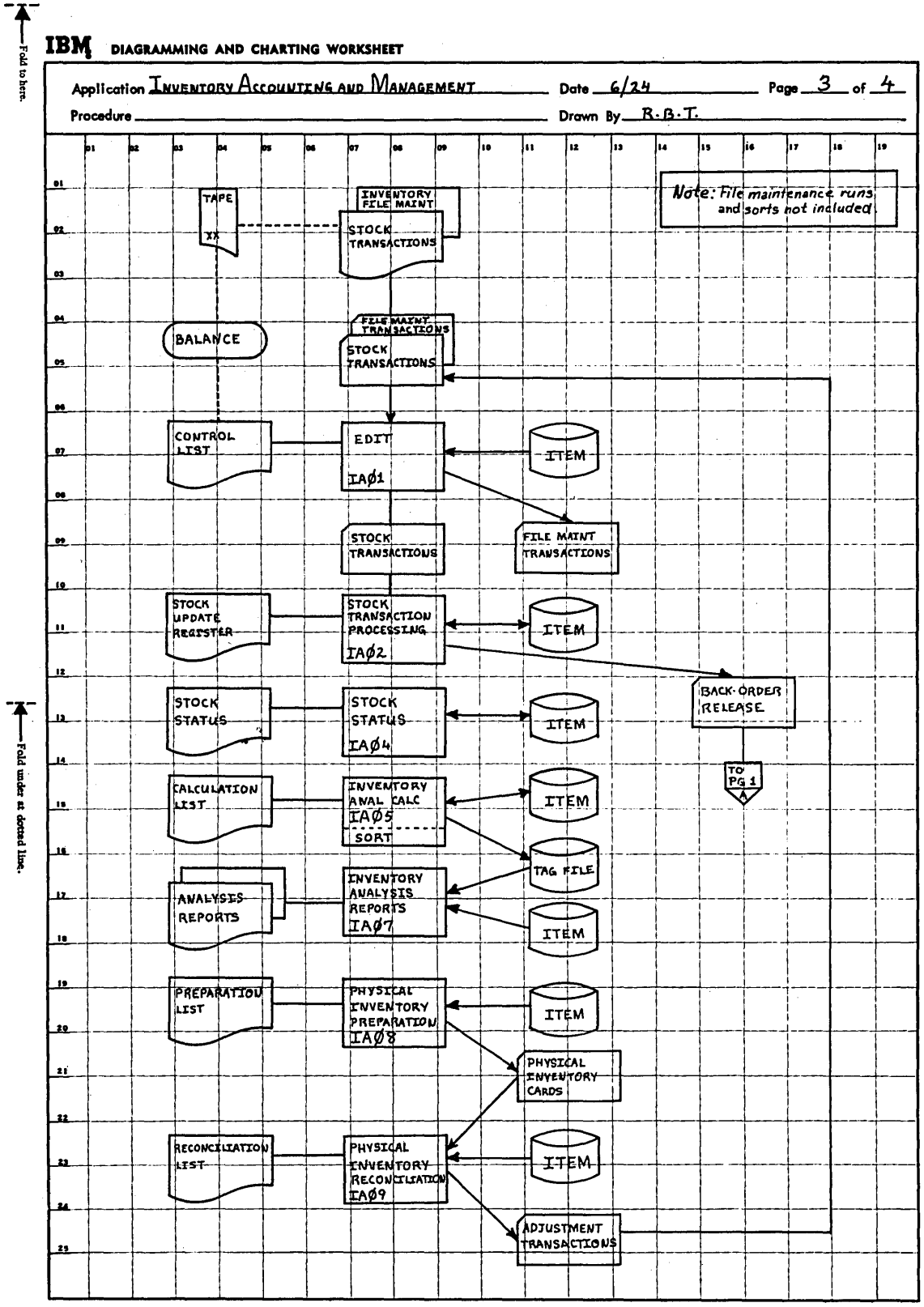


Figure 2.10C. Example General System Design–Inventory Accounting and Management

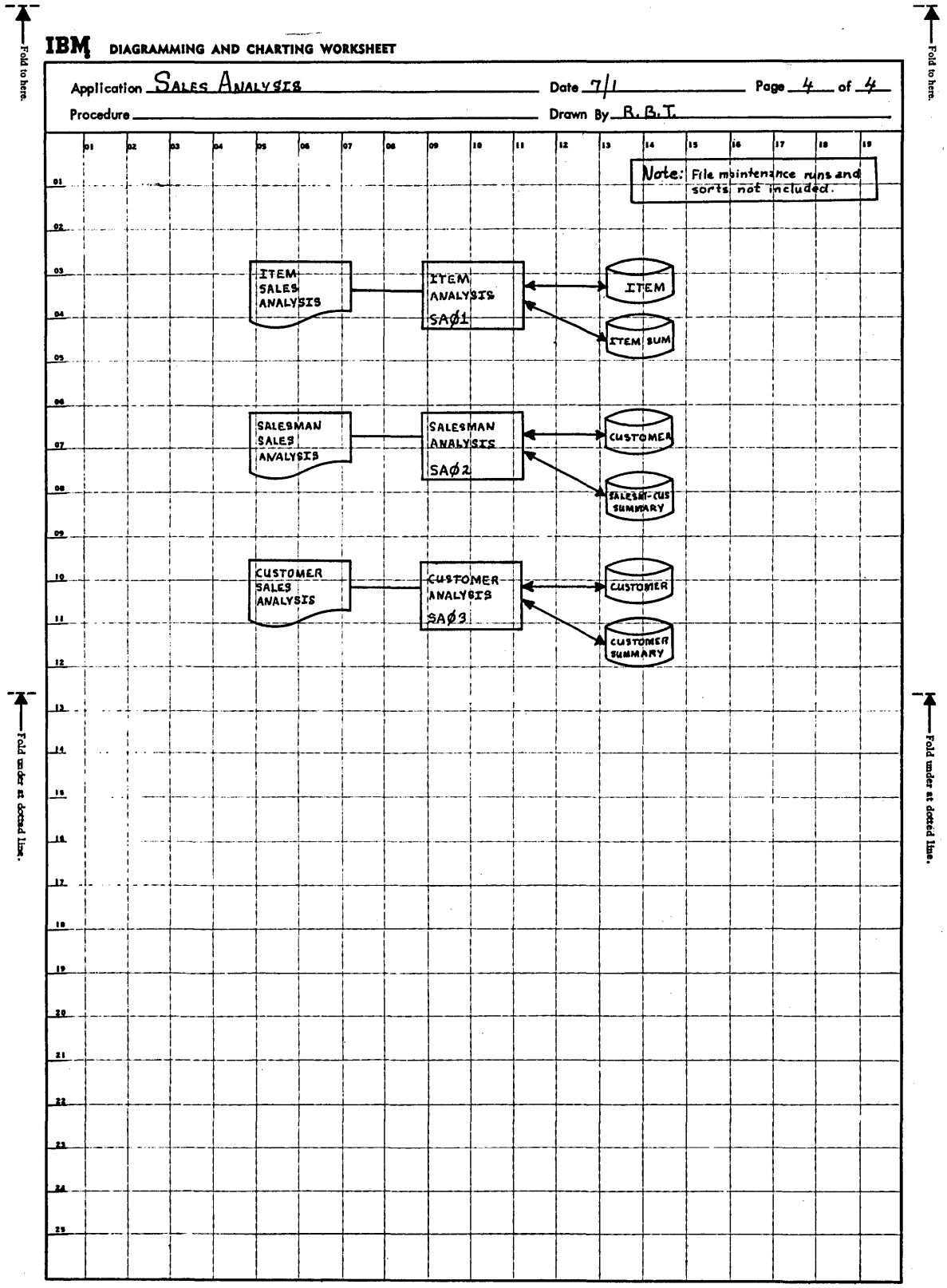


Figure 2.10D. Example General System Design–Sales Analysis

All programs needed to process the work should be named and numbered for each application. After that has been done, fill in the Application Summary form. The heading area can be filled in and the programs identified in the General Systems Design can be listed. One or more "open" programs may also be added as a buffer for each application. Each application should start a new page. (Figure 2.11 Parts A - D relate to Figures 2.10A - D)

IBM

Application Summary

Customer Name	Customer No.
SAMPLE CORP.	12345-99
Application: ORDER WRITING AND INVOICING	

Date	Page	Of
6 | 30 |	1	4
System	Model	

PROGRAM NUMBER	PROGRAM NAME	RELATIVE WEIGHT (1 TO 9)	WEEKLY POINTS / CUMULATIVE POINTS	ENTER POINTS EARNED—AS PERCENTAGE OF RELATIVE WEIGHT: DEFINE 10%	CODE & K.P./RECD. 40%	FIRST COMPILE OR TEST 10%	TESTED & DOCUMENTED 40%	REMARKS
OW01	EDIT AND BALANCE	4	Weekly	4	16	4	16	
			Cumulative	4	20	24	40	
OW02	ORDER ACKNOWLEDGEMENT	6	Weekly	6	24	6	24	
			Cumulative	6	30	36	60	
OW04	PROCESS ORDER	9	Weekly	9	36	9	36	
			Cumulative	9	45	54	90	
OW05	PRINT INVOICES	3	Weekly	3	12	3		
			Cumulative	3	15	18		
OW07	INVOICE REGISTER	6	Weekly	6	24	6		
			Cumulative	6	30	36		
OW08	COMMISSION REGISTER	4	Weekly	4	16	4		
			Cumulative	4	20	24		
OW09	BACK-ORDER PROCESSING	5	Weekly	5				
			Cumulative	5				
OW10	OPEN		Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
		42	Weekly					
			Cumulative					

Post points earned to *WEEKLY POINT AUDIT* form.

Weight Total. Accumulate. Post to Item "B" on *INSTALLATION PROGRESS POINT SUMMARY.*

G120-2314-0 UM/025* Printed in U.S.A. *No of sheets per pad may vary

Figure 2.11A. Example Application Summary—Order Writing and Invoicing

IBM **Application Summary**

Customer Name	Customer No.
SAMPLE CORP.	12345-99
Application: ACCOUNTS RECEIVABLE	

Date	Page Of
6 | 30 |	2 | 4
System	Model

PROGRAM NUMBER	PROGRAM NAME	RELATIVE WEIGHT (1 TO 9)	WEEKLY POINTS / CUMULATIVE POINTS	ENTER POINTS EARNED—AS PERCENTAGE OF RELATIVE WEIGHT: DEFINE 10%	CODE & K.P./RECD. 40%	FIRST COMPILE OR TEST 10%	TESTED & DOCUMENTED 40%	REMARKS
AR01	EDIT AND BALANCE	3	Weekly	3	12	3		
			Cumulative	3	15	18		
AR03	PROCESS + PRINT A/R REGISTER	8	Weekly	8				
			Cumulative	8				
AR04	PRINT STATEMENT	7	Weekly	7				
			Cumulative	7				
AR06	AGED RECEIVABLES REPORT	6	Weekly	6				
			Cumulative	6				
AR07	DELINQUENCY NOTICES	3	Weekly	3				
			Cumulative	3				
AR08	OPEN	5	Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
		32	Weekly					
			Cumulative					

Post points earned to *WEEKLY POINT AUDIT* form.

Weight Total. Accumulate. Post to Item "B" on *INSTALLATION PROGRESS POINT SUMMARY.*

G120-2314-0 UM/025* Printed in U.S.A. *The # of sheets per pad may vary

Figure 2.11B. Example Application Summary—Accounts Receivable

IBM

Application Summary

Customer Name	Customer No.
SAMPLE CORP.	12345-99
Application: INVENTORY ACCOUNTING + MANAGEMENT	

Date	Page Of
6 | 30	3 | 4
System	Model

PROGRAM NUMBER	PROGRAM NAME	RELATIVE WEIGHT (1 TO 9)	WEEKLY POINTS / CUMULATIVE POINTS	ENTER POINTS EARNED—AS PERCENTAGE OF RELATIVE WEIGHT: DEFINE 10%	CODE & K.P./RECD. 40%	FIRST COMPILE OR TEST 10%	TESTED & DOCUMENTED 40%	REMARKS
IAØ1	EDIT	3	Weekly	3	12	3	12	
			Cumulative	3	15	18	30	
IAØ2	STOCK TRANSACTION PROCESSING	9	Weekly	9	36	9		
			Cumulative	9	45	54		
IAØ4	STOCK STATUS	6	Weekly	6	24	6		
			Cumulative	6	30	36		
IAØ5	INVENTORY ANALYSIS CALCULATIONS	4	Weekly	4	16	4		
			Cumulative	4	20	24		
IAØ7	INVENTORY ANALYSIS REPORT	4	Weekly	4	16	4		
			Cumulative	4	20	24		
IAØ8	PHYSICAL INVENTORY REPORTING	3	Weekly	3	12	3		
			Cumulative	3	15	18		
IAØ9	PHYSICAL INVENTORY RECONCILIATION	4	Weekly	4	16			
			Cumulative	4	20			
IA1Ø	OPEN	5	Weekly					
			Cumulative					
IA11	OPEN	5	Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
		43	Weight Total. Accumulate. Post to Item "B" on *INSTALLATION PROGRESS POINT SUMMARY.*					

Post points earned to *WEEKLY POINT AUDIT* form.

G120-2314-0 UM/025* Printed in U.S.A. *No of sheets per pad may vary

IBM

Application Summary

Customer Name	Customer No.
SAMPLE CORP.	12345-99
Application: SALES ANALYSIS	

Date	Page	Of
6 | 30 |	4	4
System	Model	

PROGRAM NUMBER	PROGRAM NAME	RELATIVE WEIGHT (1 TO 9)	WEEKLY POINTS / CUMULATIVE POINTS	ENTER POINTS EARNED—AS PERCENTAGE OF RELATIVE WEIGHT: DEFINE 10%	CODE & K.P./RECD. 40%	FIRST COMPILE OR TEST 10%	TESTED & DOCUMENTED 40%	REMARKS
SAØ1	ITEM ANALYSIS	5	Weekly	5				
			Cumulative	5				
SAØ2	SALESMAN ANALYSIS	5	Weekly	5				
			Cumulative	5				
SAØ3	CUSTOMER ANALYSIS	5	Weekly	5				
			Cumulative	5				
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					
			Weekly					
			Cumulative					

Post points earned to *WEEKLY POINT AUDIT* form.

15 Weight Total. Accumulate. Post to Item "B" on *INSTALLATION PROGRESS POINT SUMMARY.*

G120-2314-0 (MM/025)* Printed in U.S.A. *The number of sheets per pad may vary

Figure 2.11D. Example Application Summary–Sales Analysis

Next, fill in the relative weight for each program. Choose a weight that seems reasonable. If a program that was assigned a weight of four turns out to require as much effort as another that was given a weight of six, the effect of inaccurate weighting will be very small.

After weight values have been assigned to all programs required by installation time, add them together and post them to item B on the Installation Progress Point Summary form as shown in Figure 2.12.

IBM

Customer Name		Customer No.
SAMPLE CORP.		12345-99
System	Model	Ship/~~Install~~ Date
		12 | 3

A. Number of weeks in Plan (to define, code, test and document) 22

B. Weight totals (total points from Application Summaries, needed prior to Install) 132

C. Average points/week needed (for on-time Install) (B ÷ A) 6.0

First "Weeks Remaining" column used should coincide with the first week of "Detail Systems Design" on Installation Planning Schedule.

"As of" Dates	/	/	/	/	/	/	/	/	7/16	7/23	7/30	8/6	8/13	8/20	8/27
Weeks Remaining	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
Points Earned This Week									0	32	44	56	85	109	65
Points Earned To Date									0	32	76	132	217	326	391
Points Needed To Date									60	120	180	240	300	360	420
Ahead of Schedule (+)															
Behind Schedule (–)									60	88	104	108	83	34	29

(continued)

"As of" Dates	9/3	9/10	9/17	9/24	10/1	10/8	10/15	10/22	10/29	11/5	11/12	11/19	11/26	12/3	12/10	12/17
Weeks Remaining	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Points Earned This Week	78	67														INSTALLATION / CONVERSION
Points Earned To Date	469	536														
Points Needed To Date	480	540	60	66	72	78	84	90	96	102	108	114	120	126	132	
Ahead of Schedule (+)																
Behind Schedule (–)	11	4														

G120-2316-1
(U/M 025)

Figure 2.12. Example Installation Progress Point Summary

Refer back to the Installation Planning Schedule and note that the detailed system design (Figure 2.9A) (item 18) begins on July 12. This is the first week in which you are able to measure progress.

Item 21, (Figure 2.9B) Program Development, extends to the week ending December 10. This is 22 weeks.

Item 30 indicates that system installation is planned for the week of December 13 - 17. The rest of this discussion will concern itself primarily with the 22 weeks from July 12 through December 10. The number of weeks is then posted to item A on the Installation Progress Point Summary, Figure 2.12.

The number of points needed per week in order to stay on schedule and install on time, can now be determined by dividing the total weight (132) by the number of weeks (22). In this case the result is six points per week.

After the above information is recorded on the Installation Progress Point Summary, the "As Of" dates and "Points Needed To-Date" can be filled in. The 7/16 date was entered above "Weeks Remaining—22". The "Weeks Remaining—1" entry is 12/10, which corresponds to the last week available for program development, prior to system installation.

Although the forms shown in this example are only partially filled out, to show how they would look after several weeks of program development, what has been explained so far amounts to the initial documentaion. Once this is done, explain what you are doing to the key executive, to obtain his agreement on the reasonableness of the measurement method. He has already agreed to the installation plan.

IBM **Weekly Point Audit**

Customer Name	Customer No.	System	Model	Page	Of
SAMPLE CORP.	12345-99			1	2

APPLICATION AND PROGRAM NUMBER	ENTER "AS OF" DATES																		
	7/16	7/23	7/30	8/6	8/13	8/20	8/27	9/3	9/10	9/17	9/24	10/1	10/8	10/15	10/22	10/29	11/5	11/12	
OWØ1		4		16	4			16											
OWØ2		6		24	6			24											
OWØ4		9			36	9			36										
OWØ5		3			12		3												
OWØ7		6				24	6												
OWØ8		4				16													
OWØ9									5										
IAØ1			3		12		3	12											
IAØ2			9			36	9												
IAØ4			6			24		6											
IAØ5			4				16		4										
IAØ7			4				16		4										
IAØ8			3				12	4	3										
IAØ9			4					16											
ARØ1			3						15										
ARØ3			8																
ARØ4				7															
ARØ6				6															
ARØ7				3															
SAØ1					5														
SAØ2					5														
SAØ3					5														
	0	32	44	56	85	109	65	78	67										

Z120-2315-0 (U/M 025)

Accumulate weekly points earned. Post to *INSTALLATION PROGRESS POINT SUMMARY* form.

Figure 2.13. Example Weekly Point Audit

Immediately following the week of 7/16, determine what progress has been made. All parties should know that you are recording the progress and that you have regular progress reviews with the key executive. This is indicated by item 16 on the Installation Planning Schedule.

To see how the points earned are recorded, look at the the Weekly Point Audit form, Figure 2.13.

All program numbers are listed on the left and the "As Of" dates across the top. More than one page may be required under actual circumstances.

In this case, no points have been earned at all during the first week of the measurement period. Some programs may have been partially defined, but not enough to get any credit. It is important *not* to give credit unless it has been earned.

So far, the Installation Progress Point Summary shows that the installation is six points behind schedule. Review this situation with the key executive and let him see the form you are using. It is a picture he can readily grasp. Explore with him why the staff is behind schedule. Perhaps IBM systems engineering services are needed. Or perhaps an education class had to be rearranged and thereby disrupted the overall schedule. In order to still install on time, several steps may have to be taken to get back on schedule.

After the week ending 7/23, the installation was measured again. You can tell by looking at the 7/23 column on the Weekly Point Audit form that "definition" of each of the six programs listed for Order Writing and Invoicing was completed. The 10% of the relative weight was recorded first on the Application Summary form, and then on the Weekly Point Audit. Again, this process takes only minutes to complete.

After all earned points are recorded on both forms, the 7/23 column on the Weekly Point Audit form is totalled (3.2) and posted to "Points Earned This Week" in the 7/23 column on the Installation Progress Point Summary. The "Points Earned To-Date" is updated (now 3.2 also), and the "Behind Schedule" field gets an entry of (8.8)—the difference between points needed to-date (12.0) and points earned to-date (3.2). No progress review is scheduled at this time.

The "cumulative" earnings should also be kept up-to-date on the Application Summary forms as points are recorded.

This can be of great value in making sure that the point count is correct. See how this works by looking ahead to the week ending 9/10.

By extracting the latest cumulative entry for each program on all the Application Summaries, one can determine that the number of points earned to-date on 9/10 is 53.6. The totals by week on the Weekly Point Audit form accumulate to the same figure of 53.6, and this agrees with the 9/10 column on the Point Summary form for "Points Earned To-Date."

The balancing of the Application Summary cumulative entries to the Audit totals is simple, avoids embarrassment resulting from hasty arithmetic, and is good data processing practice.

Go back to the time immediately following 7/30. The installation is checked again. Looking at the 7/30 column on the Audit form (Figure 2.13), you can see that the Inventory Application programs (IA01-IA09) and two Accounts Receivable programs (AR01-03) were defined by the end of that week, for an overall earning of 4.4 points. Again, these are recorded for each program, first on the Application Summary, then on the Audit form. The total earning of 4.4 points is posted to the 7/30 column on the Point Summary form, the "Points Earned To-Date" updated to 7.6, and that figure subtracted from the "Points Needed To-Date" 18.0 to arrive at the "Behind Schedule" figure of 10.4. Since six points are needed per week, the account is almost two weeks behind schedule at this time.

There is no need to worry about deferral action as yet. The progress review scheduled for that week should be held and the executive shown the Installation Progress Point Summary. Several options (assuming there are some) to get back on schedule should be discussed, and the next progress review appointment should be confirmed.

Skip to the week of 8/20. The Audit form indicates that a good deal of progress is being made at this point in time. Several programs have been coded and keypunched. This earns a healthy percentage—by design of course. A program that has been defined, coded and punched/recorded should be about 50% complete.

The total points earned during the week ending 8/20 are posted to the Point Summary, and the 8/20 column is completed. Now the installation is only 3.4

points or about half a week behind. Besides, a definite upward trend in progress and point earnings is evident.

Ideally, if this trend continued, points earned would exceed points needed. Under those conditions, and having considered all other pertinent factors, it may be desirable to discuss with the executive the possibility of improving the ship date. Remember though, that you must also improve other dates accordingly.

On the other hand, if an installation is several weeks behind schedule at the time confirmation of delivery is requested, it may be wise to consider deferral, if no alternatives are available. Bear in mind the number of "open" programs still undefined and likely to remain undefined. If the number of points behind schedule is less than this built-in buffer, deferral may be unwise.

The *trend* of points earned per week, compared to points needed per week, is highly significant.

Do your utmost to get back on schedule as soon as possible, so that loose ends can be tied up prior to system installation. This makes for a smoother conversion.

Chapter 3. Education Planning

Successful installation of a data processing system requires all personnel involved to develop additional skills and to understand the discipline imposed by the use of the system.

The education program has been carefully designed to provide comprehensive, yet selective training for your personnel in the shortest time possible. Course scheduling is flexible and instruction is paced to individual requirements.

The education program has also been designed to benefit both the experienced and the inexperienced user of data processing systems. Wherever feasible, self-study techniques have been used to minimize cost and time away from the office.

The following charts describe the product-related education available to System/3 and System/32 users. Ask your marketing representative or systems engineer for complete descriptions of each of the courses listed. They can assist you in planning the appropriate education program to meet your requirements.

COURSE MATRIX FOR THE SYSTEM/3 MODEL 4

Course	Duration	Supervisor	Prog/Imple	Operator
Introduction to System/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
Design Fundamentals for Basic Systems (D1002)	2D	R	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	R	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Models 4 and 6 Implementation (S2006)	1D	N/A	R	N/A
Communication Systems Concepts (Y2320)	2D	O	R_1	N/A
CCP Workshop (D1008)	5D	N/A	R_1	N/A
CCP Concepts & Facilities (Y5911)	3D	O	O	N/A
CCP Systems Design (D2010)	3D	N/A	R_1	N/A
RPG II 3270 Display Control Feature (D2008)	3D	N/A	R	N/A

R — Recommended O — Optional N/A -- Non-Applicable
1 — T.P. Environment Only

Although there are no formal courses, publications are available for the training and guidance of both the System/3 Model 4 system operator and for the 3270 display terminal operator.

The System/3 Model 4 system operator should plan to review the *System/3 Model 4 Operator's Guide* form No. GC21-5149, in preparation of both the Model 4 and CCP. In addition, this guide contains complete detail, halt messages, and error conditions.

Operators who will use the IBM 3270 Information Display System should review the *Operator's Guide for IBM 3270 Information System,* Form No. GA27-2742. This publication contains complete operator instructions for the 3270 System including optional devices. This manual is conveniently divided into sections that may be separated to describe the specific system and keyboard type used in your installation.

COURSE MATRIX FOR THE SYSTEM/3 MODEL 6

Course	Duration	Supervisor	Prog/Imple	Operator
Introduction to System/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
System/3 Model 6 Operation (SR20-6068)	20H	N/A	N/A	R
5496 Data Recorder Operation (SBOF-2003)	20H	N/A	N/A	O
3741/3742 Hands-On for System Implementors (SR20-4427)	6H	O	O	O
3741 Design Workshop (D2741)	2D	O	O	N/A
Introduction to Problem Solving (GC20-8097)	3H	N/A	O	N/A
S/3-6 Guide to Basic (SR29-5001)	15H	N/A	O	N/A
Design Fundamentals for Basic Systems (D1002)	2D	R	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	R	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Model 4 & 6 Implementation (S2006)	1D	N/A	R	N/A
Disk FORTRAN IV for S/3 (SBOF-2084)	24H	N/A	O	N/A

R — Recommended O — Optional N/A — Non-Applicable

COURSE MATRIX FOR THE SYSTEM/3 MODEL 8

Course	Duration	Supervisor	Prog/Imple	Operator
Introduction to S/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
3741/42 Hands-On for System Implementors (SR20-4427)	6H	R	R	R
S/3 Model 8 Operator Training (SR30-0062)	12H	N/A	N/A	R
Design Fundamentals for Basic Systems (D1002)	2D	O	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	O	R	N/A
3741 Design Workshop (D2741)	2D	R	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Subset ANS COBOL (SBOF-2083)	40H	N/A	O	N/A
Disk FORTRAN IV for the S/3 (SBOF-2084)	24H	N/A	O	N/A
S/3 Assembler Language Coding Workshop (D1006)	4D	N/A	O	N/A
Communication Systems Concepts (Y2320)	2D	O_1	R_1	N/A
CCP Concepts and Facilities (Y5911)	3D	O	O	N/A
CCP Systems Design (D2010)	3D	N/A	R_1	N/A
CCP Workshop (D1008)	5D	N/A	R_1	N/A
RPG II 3270 Display Control Feature (D2008)	3D	N/A	R	N/A

R—Recommended O—Optional N/A—Non-Applicable
1-TP Environment Only

COURSE MATRIX FOR SYSTEM/3 MODEL 10 CARD SYSTEM

Course	Duration	Supervisor	Prog/Imple	Operator
Introduction to S/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
S/3 Operation-Model 10 Card (SBOF-2001)	20H	N/A	N/A	R
5496 Data Recorder Operation (SBOF-2003)	20H	N/A	N/A	O
Design Fundamentals for Basic Systems (D1002)	2D	R	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A

R—Recommended O—Optional N/A—Non-Applicable

COURSE MATRIX FOR THE SYSTEM/3 MODEL 10 DISK SYSTEM

	Duration	Supervisor	Prog/Imple	Operator
Introduction to S/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
S/3 Operator-Model 10 Disk (SR20-6032)	10H	N/A	N/A	R
5496 Data Recorder Operation (SBOF-2003)	20H	N/A	N/A	O
3741/42 Hands-On for System Implementors (SR20-4427)	6H	O	O	O
3741 Design Workshop (D2741)	2D	O	O	N/A
Design Fundamentals for Basic Systems (D1002)	2D	O	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	O	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Subset ANS COBOL (SBOF-2083)	40H	N/A	O	N/A
Disk FORTRAN IV for the S/3 (SBOF-2084)	24H	N/A	O	N/A
S/3 Assembler Language Coding Workshop (D1006)	4D	N/A	O	N/A
Communication Systems Concepts (Y2320)	2D	O_1	R_1	N/A
CCP Systems Design (D2010)	3D	N/A	R_1	N/A
CCP Concepts & Facilities (Y5911)	3D	O	O	N/A
CCP Workshop (D1008)	5D	N/A	R_1	N/A
RPG II 3270 Display Control Feature (D2008)	3D	N/A	R	N/A

R—Recommended O—Optional N/A—Non-Applicable
1-TP Environment Only

COURSE MATRIX FOR THE SYSTEM/3 MODEL 12

Course	Duration	Supervisor	Prog/Imple.	Operator
Introduction to S/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2050)	1D	R	N/A	N/A
S/3 Operator-Model 10 Disk (SR20-6032)	10H	N/A	N/A	R
5496 Data Recorder Operation (SBOF-2003)	20H	N/A	N/A	O
3741/42 Hands-On for System Implementors (SR20-4427)	6H	O	O	O
3741 Design Workshop (D2741)	2D	O	O	N/A
Design Fundamentals for Basic Systems (D1002)	2D	O	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	O	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Subset ANS COBOL (SBOF-2083)	40H	N/A	O	N/A
Disk FORTRAN IV for the S/3 (SBOF-2084)	24H	N/A	O	N/A
S/3 Assembler Language Coding Workshop (D1006)	4D	N/A	O	N/A
Communication System Concepts (Y2320)	2D	O_1	R_1	N/A
CCP Workshop (D1008)	5D	N/A	R_1	N/A
CCP Systems Design (D2010)	3D	N/A	R_1	N/A
S/3 Model 12 Implementation (S2012)	2D	N/A	R	N/A
S/3 Model 12 Operator Training (SR30-0095)	4H	N/A	N/A	R
RPG II 3270 Display Control Feature (D2008)	3D	N/A	R	N/A

R — Recommended O — Optional N/A — Non-Applicable
1—T.P. Environment Only

COURSE MATRIX FOR THE SYSTEM/3 MODEL 15

Course	Duration	Supervisor	Prog/Imple	Operator
Introduction to S/3 Computing Systems (T1000)	1D	R	R	O
Installation Planning (Y2051)	1D	R	N/A	N/A
System/3 Operation Model 10 Disk (SR20-6032)	10H	N/A	N/A	O
S/3 Model 15 Operator Training (D1014)	3D	N/A	N/A	R
5496 Data Recorder Operation (SBOF-2003)	20H	O	N/A	O
3741/42 Hands-On for System Operators (SR20-4427)	6H	O	O	O
3741 Design Workshop (D2741)	2D	O	O	N/A
Design Fundamentals for Basic Systems (D1002)	2D	O	R	N/A
Disk Concepts & Design Considerations (D2000)	3D	N/A	R	N/A
S/3 RPG II Programming Fundamentals (SBOF-2002)	35H	N/A	R	N/A
Fundamentals of RPG II Programming (Q1005)	3D	N/A	R	N/A
S/3 RPG II Disk Programming (Q1006)	5D	N/A	R	N/A
S/3 Implementation (S2007)	4D	N/A	R	N/A
S/3 Subset ANS COBOL (SBOF-2083)	40H	N/A	O	N/A
Disk FORTRAN IV for the S/3 (SBOF-2084)	24H	N/A	O	N/A
S/3 Assembler Language Coding Workshop (D1006)	4D	N/A	O	N/A
Introduction to S/3—Model 15 (Y8016)	1D	R	N/A	N/A
S/3 Model 15 Implementation (S2015)	3D	N/A	R	N/A
CCP Concepts and Facilities (Y5911)	3D	O	O	N/A
Communication Systems Concepts (Y2320)	2D	O_1	R_1	N/A
CCP Systems Design (D2010)	3D	N/A	R_1	N/A
CCP Workshop (D1008)	5D	N/A	R_1	N/A
RPG II 3270 Display Control Feature (D2008)	3D	N/A	R	N/A

R—Recommended O—Optional N/A—Non-Applicable 1—TP Environment Only

SYSTEM/32

Class/Self Study Guide	Key	Duration	Supervisor	Prog/Imple	Operator
D.P. Concepts (Y2050)		1D	R	R	R
Installation Planning (Y2051)		1D	R	R	N/A
S/32 Operator Training (SBOF-3596)		24H	N/A	O	R
S/32 RPG II Programming (SR30-0017)		50H	N/A	R	N/A
S/32 Implementation (S2000)		5D	N/A	R	N/A
S/32 RPG II Workshop (Q2000)		5D	N/A	R	N/A
Design Fundamentals for Basic Systems (D1002)		2D	N/A	R	N/A
Disk Concepts & Design Considerations (D2000)		3D	N/A	R	N/A
S/32 SCP Utilities & RPG II Concepts (GB30-0001)		6H	N/A	O	N/A
Fundamentals of RPG II Programming (Q1005)		3D	N/A	R	N/A
3741/42 Hands-On for System Operators (SR20-4427)		6H	N/A	R	N/A
3741 Design Workshop (D2741)		2D	N/A	R	N/A
S/32 DFU Facilities and Operations (SR30-0069)		6H	O	O	N/A
WP/32 Operator Control Language Seminar **	1a	3D	R	N/A	R
WP/32 Keyboard Operator Training—Keyboard Entry (SBOF-3597)	1	10-12H	R	N/A	R
WP/32 Keyboard Operator Training—Commands & Instructions (SR30-0173)	2	30-40H	R	N/A	R
WP/32 System Operator Training (SR30-0174)	3	9-12H	R	N/A	R
WP/32 Implementation (SBOF-3595)	4	8-10H	R	N/A	N/A
Intro to S/32 Problem Solving for Commerical Users (Y5910)		1-2D	O	N/A	N/A
FORTRAN IV Fundamentals (SBOF-4024)		24H	N/A	O	N/A

R—Recommended O—Optional N/A—Non-Applicable

** This seminar which covers WP/32 commands & instructions is offered by OPD only for mag card system users and should be scheduled with the local OPD Marketing Support Rep. (MSR).

WORD PROCESSOR/32 COURSE SELECTION GUIDE

These courses should be completed in the sequence in which they are indicated.

Configuration/Audience Key to Courses

Mag Card—System/32—Word Processor/32 Application

Keyboard Operator	1a, 1
System Operator	1a, 1, 3
Supervisor	1a, 1, 3, 4

3741/42—System/32—Word Processor/32 Application

Keyboard Operator	1, 2
System Operator	1, 2, 3
Supervisor	1, 2, 3, 4

System/32—Word Processor/32 Application

Keyboard Operator	1, 2
System Operator	1, 2, 3
Supervisor	1, 2, 3, 4

Word Processor/32 Co-resident with Data Processing Applications

Select additional courses as appropriate from the System/32 Course Selection Guide above.

Chapter 4. System Design and Programming Planning

Outlined below are the critical design development tasks which must be accomplished. At a minimum, the workload and target dates for these activities should be developed and plotted on the Systems Design and Programming—Planning/Review Schedule contained in this section.

Each of the tasks described will still be applicable if you are planning to develop your own application.

TASK DEFINITIONS

1. Document Current Procedures

Obtain sample copies of source documents and printed output for all applications that will be converted. Flowchart the present system, including volumes, timings, and distribution requirements. Provide a narrative of the functions involved in these applications.

2. Determine Objectives and Develop Installation Plan

Agree on installation objectives and review the procedures for existing applications. Review the changes and improvements that will be accomplished with the new system. Schedule the activities that will be required prior to final evaluation of the new system. This schedule should include an estimated time for each activity and the number of persons assigned to each task.

3. Develop General System Design

Define the required content of the major files. Define the functions of the major runs. Define the data required in the major input records and output reports. Flowchart the overall run flow and describe the functions of the individual programs.

4. Develop Detailed System Design

Prepare detailed file descriptions and layouts, and input and output record specifications. Develop complete run descriptions describing the required functions and logic for each program. Prepare and flowchart complete run flow including all daily and periodic runs.

5. Develop Individual Program Specifications

Prepare a complete description for, and requirements of, each individual program. Use the sample chart shown in Figure 5.1 as a guide.

SYSTEMS DESIGN & PROGRAMMING – PLANNING / REVIEW SCHEDULE

APPLICATION NAME/S: _____

TASK	EST. DAYS	WEEK # / WEEK ENDG.	1	2	3	4	5	6	7	8	9	10	11	12	13
DOCUMENT CURRENT PROCEDURES		PLAN													
		ACTUAL													
DETERMINE OBJECTIVES & DEVELOP DETAIL PLAN		PLAN													
		ACTUAL													
DEVELOP GENERAL SYSTEM DESIGN		PLAN													
		ACTUAL													
DEVELOP DETAIL SYSTEM DESIGN		PLAN													
		ACTUAL													
DEVELOP INDIVIDUAL PROGRAM SPECIFICATIONS		PLAN													
		ACTUAL													
CODE, COMPILE TEST, DOCUMENT PROGRAMS		PLAN													
		ACTUAL													
DEVELOP CONVERSION PLAN		PLAN													
		ACTUAL													
CONDUCT PILOT RUN		PLAN													
		ACTUAL													
CONDUCT PARALLEL OPERATION		PLAN													
		ACTUAL													
		PLAN													
		ACTUAL													

Figure 4.1. Systems Design and Programming–Planning/Review Schedule

6. Code, Compile, Test and Document Programs

Review program specifications. Code programs. Compile programs. Define and prepare appropriate test data. Test programs. Develop complete program documentation.

7. Conversion Planning

Investigate requirements for converting source documents to files in the new system. Consider various conversion methods. Consider time factors, such as the availability of the file, the size of the file and the length of time required to convert.

Determine who will be responsible for the accurate conversion of each file, when conversion will take place, and what file maintenance will be required until the application has been fully implemented. Develop control procedures to be utilized during conversion and dual file maintenance period.

8. Conduct Pilot Run with Volume Data

User department prepares complete test data and develops required test results. Test data approximating normal volumes is run during this period, providing a basis for confirming required work schedules and setting up a daily run-book of operating procedures.

Test results are evaluated and required system corrections implemented.

9. Conduct Parallel Operation

The application is processed through both the previous and the new system. Results are compared to insure that the new system is properly processing all situations. This phase continues until it is evident that the new system is functioning correctly; The previous system may then be discontinued.

OPEN ISSUES

This section should be utilized to record unresolved issues which might affect system installation, and to describe the action required for problem resolution, the responsible individual involved and the required date for resolution.

Chapter 5. Physical Planning

This section covers important factors to be considered in preparing your offices for the installation of the system. A diagram of the actual layout of the equipment should be sketched on the grid provided in Figure 4.1. Additional information which may be required may be found in the *IBM System Installation Manual—Physical Planning.*

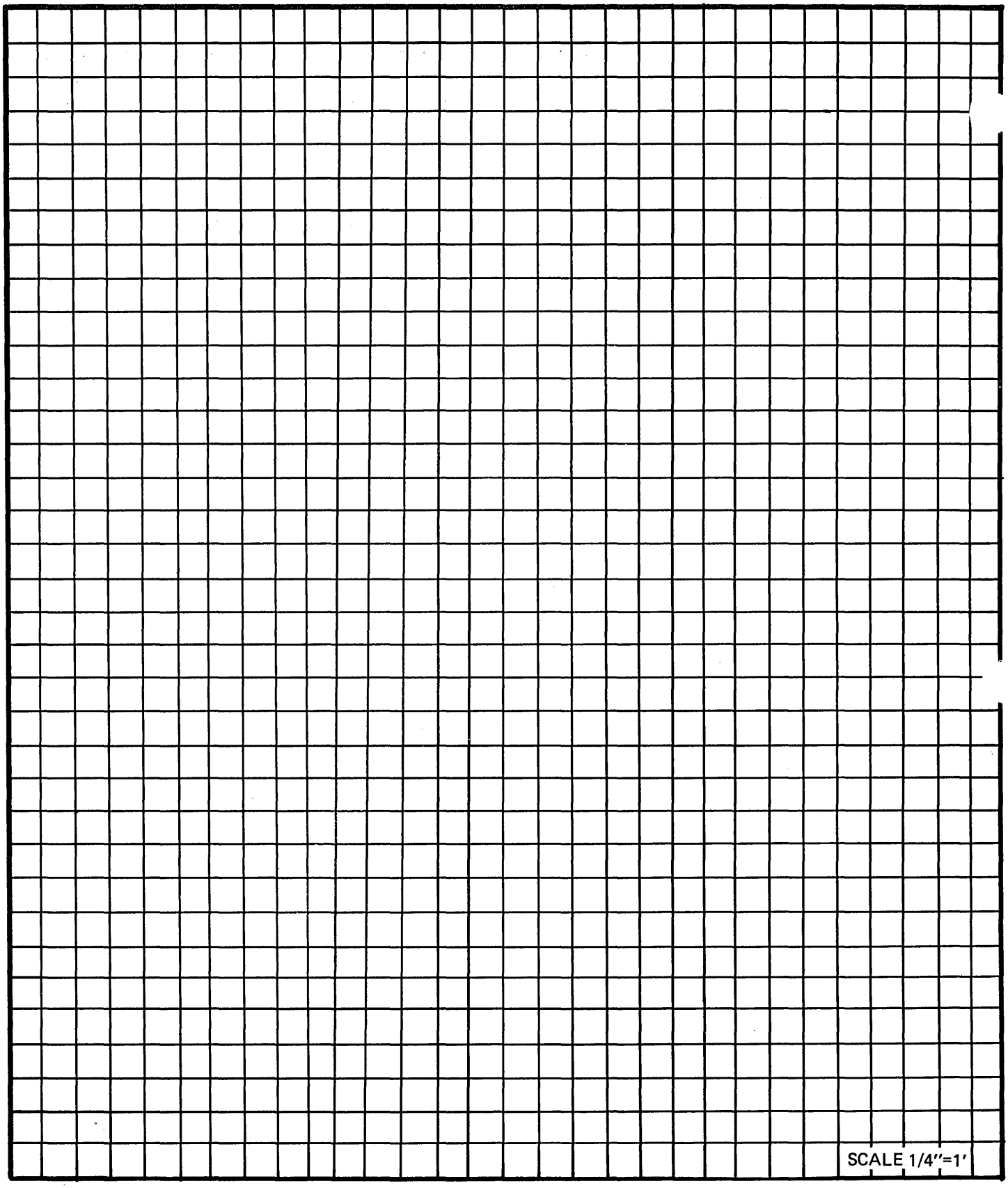


Figure 5.1. Physical Layout Planning Grid

This section lists items that should be considered when planning for the physical layout of the machine room. Since it is not possible to list all items for each customer, only those which have been found to be common to a majority of installations have been listed.

A. MACHINE ROOM

1. Machine Room Location _____ Size _____ sq. ft.
2. Construction Target Start Date __/__/__ Required Completion Date __/__/__
3. Total Machine Space Required (Check Required Machines)

Required	Type	Model	Description	Space Req'd/Unit* Width	Depth	Sq.Ft.xNo. Units	Total Sq. Ft.
_____	_____	_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____	_____	_____

Total floor space requirement for machines
(To this must be added appropriate operator and access space.)

*Includes service clearance

4. File Space Requirements

   Number of file cabinets ___x sq. ft./file _____= Total file space sq. ft. _____

5. Total machine room space required (3 and 4) _____ sq. ft.

B. ADDITIONAL SPACE REQUIREMENTS

1. Paper/supplies, disk, storage requirements

   Location in machine room _____ Other _____

   Total space required _____ sq. ft.

2. DP staff desk space requirements

   Number of individuals _____ x _____ sq. ft./person =
   (Suggest minimum of 50 sq. ft./person) _____ sq. ft.

3. Total additional space requirements (1 and 2) _____ sq. ft.

C. TOTAL DP SPACE REQUIREMENTS (A5 AND B3)

_____ sq. ft.

D. TEMPORARY SPACE REQUIRED DURING CONVERSION

Location _____

Space Required _____ Sq. Ft.

Duration Required _____ Days

Target Start Date __/__/__

Target Stop Date __/__/__

E. CUSTOMER ENGINEERING PHYSICAL PLANNING REVIEWS

Topics to be Reviewed

_____ Machine Room Layout

_____ Service Clearances

_____ Air Conditioning Requirements

_____ Power Requirements
(208/230 volts—confirm with building engineer or local power company)

_____ Machine Delivery Requirements

_____ _____ Rigging required?

_____ Elevator capacity adequate?

_____ Doorway access adequate?

F. REVIEW DATES

Schedule Review Dates

__/__/__ CE Physical Planning Representative Visit

__/__/__ Space Committed for Machine Room

__/__/__ Construction/Facilities Completed

G.AIR CONDITIONING, POWER, MACHINE WEIGHT SPECIFICATIONS (CHECK REQUIRED MACHINES)

System Specification Summary

Type	Mod	Description	Electrical		Environmental		Weight (lbs)	Notes
			kva	Conn Type	BTU/hr	cfm		(Listed at end of table)
		System/32 System/3	1.2	G	2930		640	1, 2, 3

Notes: 1. See system specifications page for service clearances.

2. Power cord is 8 feet long.

3.

Type	Plug	Connector	Receptable	Rating*
G	Hubbell or Pass and Seymour	4580	4550	208/230 volts 1 kva, 1 phase

Diagram should include the following locations:

Note: Indicate with 'NR' (not required) item not applicable to your installation.

_____ Specific IBM machines
(Use template Form GX21-9178 for System/32)

_____ Power Source

_____ Convenience Outlets
(one within 6 feet of system for CE use)

_____ Telephone/Telegraph Junction Boxes

_____ Required File Storage (diskette, etc.)

_____ Forms Storage
(If in another location, so indicate)

_____ Operator Walkspace

_____ Other Walk Areas (supervisor desk, etc.)

_____ Access Doors

_____ Fire Extinguisher

_____ IBM Customer Engineer Storage Area
(If in another location, so indicate)

_____ Manual Storage (CE and Customer)

_____ Other (Explain Below)

Chapter 6. Conversion

Thorough planning of the conversion of your applications from their present processing method to an IBM system is critical to the success of your system installation. This section defines the key elements of the conversion plan and identifies the individual responsible for these elements.

CONVERSION PLANNING

A. In-House Training

Train user departments in techniques of preparing input, and utilizing output. Review advantages to them of new system and importance of their role in success of system.

Department	Review Dates
_____	From __/__/__ to __/__/__
_____	From __/__/__ to __/__/__
_____	From __/__/__ to __/__/__

B. File Conversion Requirements

Application File	Individual/Dept. Responsible	Information Source	Physical Conversion Method	Volumes	Planned Conversion Dates
_____	_____	_____	_____	_____	__/__/__
_____	_____	_____	_____	_____	__/__/__
_____	_____	_____	_____	_____	__/__/__

C. Pilot/Parallel Plans

Application	Individual/Dept.	Target Dates
_____	_____	From __/__/__ to __/__/__
_____	_____	From __/__/__ to __/__/__
_____	_____	From __/__/__ to __/__/__

D. Control Procedure Requirements—File Conversion or Pilot/Parallel

Application/Application File	Individual/Dept. Responsible
_____	_____
_____	_____
_____	_____

E. Additional Conversion—Pilot/Parallel Manpower Requirements

Application	Function	Skill Required (e.g. Clerical, keypunching)	Estimated Man Hours
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

KEY ACTION DATES

Successful installation of your system will require that decisions be made and action taken at certain important junctions during the installation program. Contained in this section are many events which will require action with specific target dates established.

A. Education Enrollments

Student Name	Student Function	Individual Responsible	Target Enrollment Date
_____	*Customer Executive*	_____	__/__/__
_____	*Installation Manager*	_____	__/__/__
_____	*Programmer*	_____	__/__/__
_____	*Operator*	_____	__/__/__
_____	_____	_____	__/__/__

B. Commit D.P. Staff

Individual's Name	Position/ Function	Individual Responsible	Target Assignment Date
_____	*Installation Manager*	_____	__/__/__
_____	*Programmer*	_____	__/__/__
_____	*Operator*	_____	__/__/__
_____	_____	_____	__/__/__
_____	*Conversion Personnel*	_____	__/__/__

C. Physical Planning

Activity	Individual Responsible	Target Action Date
Space Committed	_____	__/__/__
Contractor Engaged	_____	__/__/__
Power/Air Conditioning—		
Reviewed/Approved	_____	__/__/__
Physical Machine Delivery—		
Reviewed/Approved	_____	__/__/__
Construction Completed	_____	__/__/__

D. Order Program Products and Industry Application Programs*

Program Products	Target Order Date	Industry Application Programs	Target Order Date
Utilities (MCL,DFU, SEU,SORT)			
_____	__/__/__	_____	__/__/__
RPG II			
_____	__/__/__	_____	__/__/__
_____	__/__/__	_____	__/__/__
_____	__/__/__	_____	__/__/__

*System Control Program Shipped with System

E. Conduct In-House Training

Application	Department Name	Target Training Date
_____	_____	__/__
_____	_____	__/__
_____	_____	__/__

F. Sign Systems Engineering Estimates (If Required)

Scope of Effort	Individual Responsibile	Target Order Date
_____	_____	__/__/
_____	_____	__/__/
_____	_____	__/__/

G.Order Forms/Supplies

Form Name	Individual Responsible	Target Order Date
_____	_____	__/__/
_____	_____	__/__/

H.Order Storage Equipment

Equipment Required	Individual Responsible	Target Order Date
Files _____	_____	__/__/
Diskette Cabinets _____	_____	__/__/
_____	_____	__/__/

I. Final Approval of Conversion Plans and Procedures

Application	Individual Responsible	Target Approval Date
_____	_____	__/__/
_____	_____	__/__/
_____	_____	__/__/
_____	_____	__/__/

REVIEW MEETINGS DATES

This section describes a series of review meetings organized in a sequence corresponding to the occurrence of key events during the installation program. The meetings should be scheduled to review progress in keeping with the target dates established in the section on Overall Installation Plans. Additional meetings should be scheduled at appropriate intervals to review progress on the system and programming (maximum two week intervals are suggested) if you are planning to write your own applications.

Suggested Review Meeting Schedule

Meeting Number	Topics for Review/ Action	Suggested Participants	Scheduled Date	Action Required/ Taken
1	Commit DP Staff Review/Approve Education Enrollments Identify/Commit Required Space	Customer Executive IBM Representative	__/__/__	
2	Review/Approve Package Fit. Review/Order Program Products and Applications	Customer Executive Customer Installation Manager IBM Representative	__/__/__	
3	Review/Approve Package Fit. Review/Order Program Products and Applications	Customer Executive Customer Installation Manager IBM Representative	__/__/__	
3	Review/Approve Physical Planning • Engage Contractor • Power/Air Conditioning • Machine Room Layout • Phsyical Delivery Requirements	Customer Installation Manager Customer Technician IBM Representative IBM Field Engineer	__/__/__	
4	*Approve/Finalize Systems Design	Customer Executive Customer Installation Manager IBM Manager IBM Representative	__/__/__	
5	Approve/Order Forms, Supplies, Diskettes, etc. Approve/Order Storage Equipment	Customer Installation Manager	__/__/__	

* Customers who are writing their own applications.

Meeting Number	Topics for Review/ Action	Suggested Participants	Scheduled Date	Action Required/ Taken
6	Review/Finalize Conversion Plans and Procedures Review/Approve Progress on Machine Room Preparations	Customer Installation Manager IBM Representative	__/__/__	
7	Post Installation Review of Volume, Statutory, or Other Changes to System; Consider Extension to New Application Areas.	Customer Executive Customer Installation Manager IBM Representative	__/__/__	

Post Installation Review and Future Plans

This section defines activities to occur after your system is installed.

A. Identify Required Additions and Modifications to Systems

Application	Requirement	Individual Responsible	Target Completion Date

B. Develop Plan for Automation of Additional Applications

Application	Responsible	Amount of SES Required	Target Completion Date

Chapter 7. Considerations of Data Security in a Computer Environment

INTRODUCTION

Only the customer can determine the level of protection sufficient for his company's needs. However, this section is a guide to provide general management, systems personnel and operations management with various data security considerations in order to assess and minimize potential problems. It does not, however, attempt to cover highly classified systems within the government—those with stringent requirements peculiar to data involving the nation's security.

The section discusses considerations of data security necessary when computing systems store and process either proprietary data or personal information on individuals. While it does not cover the much broader social issue of privacy, it does proceed with a recognition that the protection of individual privacy places special responsibilities on those who determine how systems are to be used.

The addition of remotely located terminal devices significantly increases the potential problems and the resulting concern for data security. Problems range from preventing the curious intruder from browsing through personnel rosters, customer lists, operating statements, etc., to preventing the malicious intruder from altering payroll records, obtaining secret financial data or illegally obtaining copies of new product specifications.

Working Definition

Data security can be defined as the protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modification. Techniques for security include computer hardware features, programmer routines and manual procedures, as well as the usual physical means of safeguarding the environment with security personnel, locks, keys and badges.

Data Security and Advancing Technology

The need for data security exists whether the information is in manila folders in the personnel file, in a deck of punched cards in the payroll departments, in a small computer system, or in the data bank of an online communications-oriented system. Information may be equally useful or equally damaging whether it is obtained from a manila folder, a file cabinet, a safe or a terminal connected to a computer.

The current and increasing concern for data security is the result of three major interrelated factors.

The first is the dramatic technological advancement in computing hardware and programming systems. Today, multiple jobs and/or multiple users can

concurrently access the system's facilities and its stored data. Computation speeds are in millions of operations per second, and the amount of data stored online can be in the billions of characters—any accessible in a fraction of a second. Each of these independent jobs or users may have been assigned widely varying security authorizations and the data elements themselves may have diverse requirements for protection.

The second factor is the ever-growing need of business, science, industry and government for processing larger and larger quantities of data as rapidly as possible. As the per-unit cost of both data processing and storage decreases, it becomes economically feasible to attempt whole new areas of analysis.

The trend is for more and more information to be learned and data to be gathered from the scientific experiments in our laboratories and hospitals; the social experiments in our towns and cities; our struggles with the elements on land, sea and air; the performance of our machines and appliances; the weaponry and strategies of our armies and those of our enemies; the survival of our astronauts; the strength and growth of our economies.

The third factor, the result of greater availability of digital communications facilities and terminal devices, is the increasing emphasis on providing "computing power" at the remote operations levels.

Much of the computer design effort in recent years—both in hardware systems and programming—has been devoted to making it as easy for the non-computer-oriented individual to compute on a small system or from a terminal as it is for the non-automotive engineer to drive a car. Many systems provide guidance and computer-assisted instruction to help the new user quickly become productive. In addition, because many of these systems directly affect the public, demonstrations showing exactly how the system works have become a natural part of system implementation.

These developments, coupled with computing systems advances, have led to implementation of systems which permit the bank teller to verify and update an account balance, the reservations agent to confirm the details of a trip, the department store clerk to obtain instant credit information, the order clerk to know the on-hand inventory and be able to trace shipments, the programmer to develop and test new applications, the policeman to know if a car is stolen—for people in general to be able to do their jobs better and faster with more current, usable information.

The benefits derived from these uses of computing systems are dramatic. However, as access to information is extended outward to operating levels, security measures must correspondingly extend outward to control this access.

Design Considerations

The major challenge is to develop procedures and to identify and employ operational techniques which will help appropriately safeguard private information, preventing its indiscriminate release or unauthorized modification.

No two organizations have either identical requirements for security or identical facilities for implementing their requirements. This precludes the development of a single standardized solution. But it also makes it more difficult for the intruder to develop a "cookbook" on how to breach a specific user's security system.

Solutions to the data security problem are being found by combining 1) the normal accounting control procedure of separating responsibilities among personnel, 2) traditional physical security measures of locked doors, identification cards, operating procedures and trustworthy personnel and 3) the capabilities of the computing system itself. Hardware features such as storage protection, recognition of interrupts, separation of problem and control program states in the central processor, plus programming systems features such as password verification, label and data checking, etc., exist in many systems today. By evaluating the applicability of these and by knowing the requirements of his own data processing application, the users can help minimize potential problems by programming significantly more comprehensive security checks than were possible with manual systems. For example:

1. Consistent verifications of both identification and authorization of the individual user location and/or terminal, depending on the degree of security required, *each time* an attempt is made to access restricted data.
2. Immediate detection of any accidental or intentional security breaches. Identification of the time of the breach and the person responsible; and, if needed, cancellation of that program and/or disconnection of that terminal or inquiry device.
3. Maintenance of detailed records of *all* accesses to sensitive data files and by subsequent computer analysis of user, terminal, location, level of authorization, type of errors, etc., measurement of the effectiveness of security techniques.

The data security area is not unlike most other major functional areas of business. General management provides direction—setting policy and establishes goals. Middle management and the systems specialists provide design—building into the system the ability to obtain the required security. Operations management provides implementation—maintaining and enforcing the procedures under which security can flourish.

The remainder of this section discusses the various facets of data security as they are the concern of general management, the systems design function and data processing operations management, be they separate or the combined functions of one individual. The concluding pages contain "42 Suggestions for Improving Security in Data Processing Operations."

SECURITY CONSIDERATIONS FOR GENERAL MANAGEMENT

In reviewing each application, management's traditional concern has been to establish policies to protect against *loss* of any vital data stored and processed. Vital data was defined in terms of protection of the equities of the owners, employees and customers, or as data needed to enable the organization to go back into business within a reasonable period of time following a disaster. "Disasters" meant not only nature's calamities, but also equipment failures and both the accidental and malicious acts of people.

Policies and procedures have evolved which minimize the problems posed by the computerization of vital data. Today's critical concern arises from storing and processing that additional proprietary or personal data considered sensitive.

If certain data were disclosed to unauthorized persons inside or outside the company, would it be embarrassing, would it benefit competitors, would it hinder contract negotiations, or would it violate company policies? Specifically, *data security measures are needed to prevent disclosure to or modification by unauthorized persons.* The information requiring this special protection logically *includes* all *data* which *management considers proprietary.*

Personal data, often compiled from external sources, must also be protected. This may include employee personnel information such as medical histories, credit investigations, performance records and salary schedules.

Interrelated Factors

Key factors to be considered in determining the nature and extent of the protection required against disclosure are:

- The application or system's function (online banking, new product design, payroll, financial data, etc.) or combination of functions.
- The equipment configuration (local batch processing, in-house terminals, remote terminals and/or processors).
- The degree of data sensitivity (the anticipated consequences of disclosure or modification).

The manager's decision on security requirements is based on the trade-offs among these factors plus consideration for the cost of security, which can involve:

- Hardware, ranging from additional computer equipment to vaults for storage or key locks on terminal devices.
- Restrictions on use—essentially a negative factor that measures how much more broadly useful the system might be were data security not a factor.
- Reduced system efficiency resulting from use of various identification, authorization and audit procedures.

There are *no simple formulas* for examining the cost-value trade-offs in applying data security measures. Even when all significant quantitative factors can be assessed, subjective criteria will often exert greater influence over what is actually done about security. In particular, consideration must be given to:

- *Employee Loyalty and Judgment.* If access to the system, the terminal and the sensitive data can be controlled so that only persons of good judgment are involved, and if those persons are, in fact, loyal, there will be fewer possible avenues for loss of security.
- *The Involvement of Outsiders.* Many people participate in data processing: auditors, consultants, representatives of hardware and software vendors and communications company employees. In addition, the general public is introduced by seminars, demonstrations, and open houses. The exposure represented by these non-employees may require additional effort to develop adequate precautions against unauthorized disclosure.
- *Experience with Security.* Within a company that is familiar with security administration and the control of confidential company documents, the addition of new sensitive data may have only a minor impact.

Review Techniques

The security procedures of any given system or installation are unique to its specific needs. Regardless of which security measures are employed, one of the most important elements in any successful data security program is that it be tested and audited regularly and at random intervals.

The tests should be constructed with a conscious effort to breach the system's security, not merely to validate the existence of the techniques. The normal audit function is to analyze the activity log, transaction summaries and control figures for any unusual activity or any suspicious patterns.

In addition, the audit of data security measures should provide a review of:

1. *Current Effectiveness.* Do security breaches occur; are the testing programs and procedures up to date; how recently were they run; did the runs result in security changes; were the changes incorporated and documented and therefore, is a new test planned?
2. *Continuing Appropriateness.* Are the data still considered sensitive; are there the same potential consequences of disclosure; are there other new management policies to apply? Are the original criteria used in assigning identification cards, passwords and keys still valid? Are new methods of protection available?
3. *Level of Complexity.* Are controls excessive or are they less than required for adequate cost-effective security? Is it *necessary* to maintain a 100 percent detailed audit trail containing every access to specified pieces of data and to record the identity of each user who requested, processed or altered that data, and the time of that action?
4. *Staff Assignments.* Do checks and balances exist so that no one person or department can compromise security? Are job assignments rotated to

prevent familiarity from encouraging laxity? Are similar guidelines applied to the data processing and security administration areas?

5. *Training.* Have techniques to bypass security evolved in order to simplify the training of new system's users? Are penalties for violations clearly outlined? Do demonstration programs allow the knowledgeable user freedom to browse?

6. *Special Reports.* Does this system delete sensitive data when responding to legitimate requests for information from outside groups? Do special programs exist which circumvent security in order to meet special format requirements or deadlines?

The decision to implement any given set of data security techniques depends on the foregoing considerations plus the policy guidelines and "atmosphere of concern" provided by general management. Within that framework, the functional area or manager assigned responsibilities for the data must clearly and realistically identify those data elements which require special precautions or protection.

SECURITY CONSIDERATIONS FOR SYSTEMS DESIGNERS

The systems designer or lead programmer contributes to security by capitalizing on the facilities of the computing system in order to augment the external manual procedures. Specifically, he can design and program more elaborate, more precise and more consistent controls over selective access to sensitive data. These controls, coupled with personnel, procedural and physical measures taken by operations management, can significantly reduce an organization's exposure to potential data security problems.

Security systems must be modular and also optional, so that security procedures are tailored to the user's *needs* and not forced into inappropriate areas. *To guard against "over-security," a technique should be devised to determine the complexity created by security measures and relate that complexity to both performance loss and actual need for security.*

Key factors which influence design of a secure system are:

1. Information content, where the data may require:
   a. No special security provisions
   b. Normal need-to-know restrictions
   c. Extensive precautions to avoid disclosure
2. Environment, where users may be:
   a. All online, all offline or in any combination
   b. Equal or widely varying in security clearances
3. Communications, where devices and activities may be:
   a. Local (within the same building or operating complex)
   b. Dedicated, private network
   c. Switched network

4. System facilities, where the services provided may be:
   a. Dedicated function only—inquiry or data entry
   b. Interactive problem-solving
   c. Full remote programming and testing support
   d. A total information system

The controls then developed must be assessed in terms of the specific user orientation of each system. The system's orientation to the people who will use it, the terminals, if any, which will access it, the transactions it will process or some combination of these determines which actual operating procedures will best contribute to meeting security requirements.

Identification

Based on the degree of security required, either the person, the terminal or the program attempting to access sensitive data should be identified so that the right to use the system or function can be verified and the user can be held accountable. For example, if everyone in a city welfare department may access that department's file, the terminal need only be physically located and secure in the welfare office. Then the only additional requirement is a means of uniquely identifying that terminal to the system or otherwise assuring the system that the output is directed to the correct terminal.

But if only one or two individuals among many people are authorized access, for example, to adoption records, there must be a means of ascertaining who is requesting adoption records.

Degree of Protection

The search for greater security should be balanced against the risk of being too elaborate and therefore dollars, time and system consuming. In addition, as new users or applications are added to the system, the basic identification philosophy should be reviewed. How little information and verification is needed to be reasonably certain of the user's identity? How cumbersome or complex has user training become?

The final concern in any approach chosen is that both the program logic routines and any stored tables require an extra measure of protection. In some systems, they are treated as an integral part of the control system. All testing, additions, changes, and deletions to these data sets are restricted through the use of another password available only to the security administration officer.

Design of Authorization Techniques

Once the user is identified, the system must determine what he is authorized to do. He may be authorized to use some programs or functions, but not all. He may be authorized access to certain files, but not others. He may be permitted to read certain files, but not modify them.

Therefore, a table identifying each user's authorizations is needed. On some systems, the authorization procedure will be quite simple. On others, it will be highly structured and complex. How simple or how complex depends on what capabilities the system provides and how selectively these capabilities are provided to various users.

In simplest form, system users are divided into a small number of categories. The user's ability to access various application programs, files, etc., will depend on his category. The category can be identified to the computer by the device used to sign on—password, badge, key, terminal address or terminal type.

On some airline systems, the card with which a user signs on indicates his category. He is a supervisor, reservation clerk, trainee, demonstrator, etc. Similarly, on many banking systems, a special key inserted in the terminal identifies the user's authorization to access more than routine data.

In other systems, the authorization must be specific to the individual himself. In this case, a table relating specific authorization to specific user is needed.

At times, rather than using a single authorization category, the authorization table requires structuring according to application programs or transaction types. The table would then list each user and identify each transaction or program authorized to him. It would be inspected either at sign-on time or immediately preceding execution of any transaction or program.

But it may be necessary to further segment this authorization. For example, entry of the transaction code in the user's record could be a "read only" authorization. Adding a suffix digit to the authorization table entry would permit control of read only, update only or various combinations. An additional suffix digit could designate the user's training status. (He may have the authority by virtue of job level, but lack sufficient training with that transaction type.) Much more elaborate schemes are even possible.

Since the authorization table is the master key controlling the processes and transactions that can be accomplished, its security is, of course, critical. Changes to these authorizations must be initiated by management and must be treated as sensitive data. Such changes should be reflected in all logs and subject to regular and random review by the executive security officer, auditor or key executive.

SECURITY CONSIDERATIONS FOR OPERATIONS MANAGEMENT

The systems design and operations management aspects of a secure data processing installation are almost totally interdependent. Unless operations management maintains physical, procedural and personnel safeguards, the system's security will constantly be at risk, no matter how much protection has been programmed in.

Physical Security

The central computing facility, its related tape/disk libraries, the data preparation area and the supporting clerical control departments should be considered as one unit for security purposes.

A secure data processing system may need physical guards on the computer center, possibly also on some terminal locations. It may need a security staff to keep intruders out, assure that tape or disk stores are locked and perform periodic inspections.

The ready availability of cameras, microphones and other accouterments of eavesdropping requires that consideration be given to the physical location of such system components as main console, terminals, and printers. Both the casual viewer at an open door and the more sophisticated intruder with a telephoto lens or parabolic microphone can be deterred when system components are kept away from open windows, doors and the glass walls that frequently surround machine rooms.

Physical access to the computer room should also be restricted to only those people actually engaged in support of computer operations. At least one senior person per shift should be designated responsible and accountable for maintaining security precautions.

Locked cabinets or vaults should be used to store sensitive data files, backup files, associated operating procedures and documentation. The tape and disk librarian should maintain a log that records, at a minimum, exactly when and by whom sensitive material is removed and returned.

Program decks, documentation, test cases, sample outputs and procedures which operate on sensitive data should be treated as securely as the data themselves. To avoid the possibility of both error and loss of security, prior versions of such material should be clearly labelled, held secure and then destroyed as soon as the new system is fully operational.

Operating Procedures

Security routines are often programmed as integral parts of the operating system's control program, application program, access methods and data management. Therefore, procedures are needed to verify that the system is intact after all changes, customer engineering activity and testing sessions. The procedures should be employed as a normal part of the daily start-up and close-down of the system, as well as after any system outage requiring recovery and restart.

Logs should be maintained to record each running of a sensitive job. These should report any significant action taken, such as an operator decision to override tape/disk labels or passwords.

Program testing aids and procedures are normally designed to provide the maximum information possible to facilitate debugging. The presence of sensitive data, either online or offline but accessible, may require restrictions on full storage printouts, on the use of standalone utilities which modify files and on requests for file dumps that may compromise the security of data within the system. (A major concern is that standalone programs are, by their nature, independent of controls built into the operating system.) In some highly secure systems, program testing is permitted only with artificial data and only when actual data is physically offline.

Both manual and computer restart and recovery procedures should be designed so that checkpoints, core dumps, and/or the entire restart procedure do not provide a road map to the system's security controls.

Demonstration programs also, whenever practicable, should be limited to data sets containing artificial data, to prevent not only disclosure of sensitive data, but possible loss due to errors.

If necessary, the demonstrations themselves, whether at remote terminals or within the computer facility, should be limited to an audience with a need to know.

Personnel

Maintenance of security demands competence, loyalty and integrity from systems operators and machine room personnel. In addition, it requires continuing training for them, both in operating procedures and security measures. The purpose of this training is to insure that each individual recognizes his vital role in installation security and does not—through familiarity—become careless.

No one, regardless of level of competence or job responsibility, should be able to circumvent the security procedures, logs and audit trail.

The control of employees of other departments, as well as outsiders, may require special precautions such as sign-in registers, badges or special escorts. As computing systems and peripheral devices become increasingly more complex, the nature and variety of these outsiders expands significantly beyond those who traditionally participate in data processing. And usually these people are most deeply involved during times of crisis—a conversion or a system malfunction—when the urge to bypass security in order to get the system operational is very great and must be resisted.

Success in managing a secure installation is only possible through consistent and continuous adherence to the security measures. All indications of both successful and attempted violations must appear on the logs and audit trail. The review of these should be a combined effort by operations management, systems design and the security officer to determine and implement whatever improvements the system may require—physical, procedural, personnel or programming.

42 SUGGESTIONS FOR IMPROVING SECURITY IN DATA PROCESSING OPERATIONS

Organizations that use data processing equipment maintain some kind of physical security. Whether they lock up their punched cards, maintain backup files on data in-process, or simply keep track of visitors, their need for physical security is a fact of life.

No set of rules and procedures can guarantee total physical security for data processing operations. But there are some basic things you can do about the more obvious security problems.

The 42 suggestions offered here cover some of the problems of physical security most commonly encountered today. They do not represent a checklist. But they are based on observations and comments by people who are experienced in operating data processing installations. They may be helpful to you in evaluating present physical security measures or in designing an improved physical security system.

1

Control access to the system area.

Few installations provide more than minimal protection against people who may want to steal punched cards, magnetic storage media, paper output or who may try to damage the hardware.

Maintaining the physical security of your system area is your first line of defense. But only you can decide how much security is enough. This means taking into consideration the value of the data to you, the cost of its protection, the impact its loss would have on your organization, and the motivation, competence and opportunities of those who might damage the data or the system.

2

Define responsibilities for the security of data, systems, and programs.

Data, systems, and programs are assets, just as the more tangible hardware units and your physical plant are. Specific responsibilities for their protection should be firmly established if adequate security is to be achieved. It is relatively rare to see an operation where the fundamental responsibilities for the security of the data in the system are crisply stated and broadly understood.

In general, the person with physical control of an asset should have the immediate responsibility for its protection. In the case of data within the DP center, this person is the center's manager. Data and programs located elsewhere should be the responsibility of the people in charge of those locations.

Internal auditors and your security staff should review the adequacy of the protection given the data. Because they do not have physical control over it, however, they generally cannot be given the primary responsibility for its safety.

3

Involve a number of people in sensitive functions.

To the degree permitted by the scale of your operations, the duties of writing, running and authorizing a program, job, or especially a change, should be assigned to different people. Effective separation of related sensitive functions will help reduce error and lessen the risk of deliberate unauthorized acts by the staff.

An audit trail should be maintained so that management can track functions to ensure that each person is performing his assigned role. For example, management might compare console log entries to the production work orders to determine whether the operator was authorized to run each and every job that was run.

4

Indoctrinate data processing personnel with the importance of security and their individual responsibilities in achieving it.

When a system is being used for only one function such as inventory control or order entry, the people associated with the system's operation generally feel specific responsibility or reasonably strong motivation to protect the data and produce the desired end results. However, if a center supports a number of different operations, personnel operating that center are often unaware of the implications of disclosure, loss of destruction of data in each of the diverse functional areas that they support.

No security measures can be effective without the support of most operating personnel. People generally respond well when they're aware that they occupy positions of great trust and responsibility. Their alert, enthusiastic support of the security measures which are put in place is necessary for you to achieve any significant degree of security.

5

Maintain a data inventory or other measure of the value of your data holdings.

It's not easy to make a sound determination of the need for security measures, or to justify not applying them, unless you've made quantitative assessment of the value of the data being protected. The proposal to put a dollar value on data on a file-by-file basis is generally greeted with considerable skepticism. But data and programs are assets with determinable values. Making the assessment is feasible in most cases, and quite often produces rather surprising results.

An evaluation of your data holdings should take into consideration all the things that can happen to data: accidental or intentional disclosure, modification, loss, or destruction. Once this is done, it is often possible to make reasonable judgments of the value of the data to you and the cost of protecting it. This, in turn, can be weighed against its possible value to others and their cost of

acquiring it. This should enable you to make a reasonable decision as to what security measures are appropriate in the light of their effectiveness and cost.

6

Take prompt, decisive, corrective action when security is jeopardized or lost.

If corrective measures aren't taken when a few people disregard established security procedures, other employees may assume that management isn't very serious about security. Well-conceived and normally effective security measures become ineffective when people find that they can be circumvented or ignored with impunity. This is particularly true when security measures are ignored or openly ridiculed by senior personnel and management.

7

Protect yourself against the destructive activities of disgruntled personnel.

There are a number of instances in which employees who were recently discharged, or who knew that they were about to be discharged, have destroyed files or modified them for their future benefit. For example, they've added their name to the pension rolls or generated an excessively large severance paycheck.

Protect yourself by setting up procedures to promptly and completely exclude all disgruntled, disaffected people, particularly those with special knowledge of the system. Dont't give them any opportunity to damage or otherwise modify the files or the physical facility.

8

Assess threats to your data holdings.

Frequently, management shows great, often temporary, concern for well-publicized, exotic physical security problems. A significant percentage of these never occur, at least not in the manner described. Less frequently, unfortunately, management makes a reasonably thorough analysis of the susceptibility of a facility to the rather wide variety of things which may occur.

Such an analysis often leads to the rejection of many things previously considered to be problems and the inclusion of others which are quite important but less obvious. In short, to establish a rational program for the protection of an asset, you should determine the value of the asset, as described before, and the threats to it, as noted here.

9

Set up emergency security procedures.

Normal security procedures sometimes have to be modified when an emergency such as a tight deadline or system malfunction occurs. You can maintain the integrity of your security procedures at such times by using extra management supervision.

To minimize exposure associated with out-of-the-ordinary events, set up emergency procedures that require more-than-usual management supervision and management participation in each key decision. Procedures should also include provision for documenting the event, authorizing the substitution of emergency security procedures for normal ones, and for performing all the actions taken while the emergency situation exists.

10

Be realistic; don't operate in reaction mode only.

In some organizations, security measures have been incorporated primarily in reaction to well-publicized problems encountered by others. This has frequently led to illogical responses to situations which frequently did not exist or which were so inaccurately described as to be grossly misleading. Included in this category are the magnets carried into the machine room which resulted in the erasure of all magnetic media in the area, the erasure of tapes and packs by airborne radar, and the acquisition of proprietary business information by vans parked outside bristling with antennas and microphones eavesdropping on the computer.

Concern for the loss of data in these rather elegant ways can completely mislead management so that it ignores more usual, everyday situations such as the pile of proprietary information lying on the loading platform waiting for the trash man.

11

Don't identify your data processing centers.

Data processing facilities sometimes appear to attract the ire of potentially destructive groups of people, because those people associate computing with major national issues such as military conflicts, pollution, credit data banks and other sensitive topics. Other facilities with no immediate association with such issues, but which are physically located in the same general area, should also be concerned for the safety of their data processing installations. Computing installations are, in the minds of many, the ultimate symbol of the Establishment. If there are two potential targets to draw the attention of destructive people in an area, it is probable that they will take on the one whose location is known to them as opposed to disrupting the one whose location has to be determined with some effort.

12

Carefully select and implement fire detection and quenching systems and their interconnections, if any, with electrical power.

Fire detection and quenching systems should be selected and installed in the light of realistic, well-informed assessments of the risks, the costs, and the possible sources of fire. Evaluate new detection and quenching systems as they become available.

Also, consider how these detection and quenching systems will be integrated with your electrical power. This will save initial system installation costs and, with some quenching systems, damage from water in the event of fire. In short, fire detection and quenching systems should be selected with guidance from well-informed, objective experts in that field.

More consideration should also be given to the use of fire-retardant walls around areas you want to protect from fires that might originate in nearby areas.

13

Check the vulnerability of your air-conditioning installations.

Many DP center air-conditioning installations reveal that inadequate concern has been shown for the locations of their fresh air intakes. Considerable disruption or damage could be caused, accidentally or intentionally, by the ingestion of undesirable gases and vapors into them. The list of things which should never be near fresh air intakes is quite long, and it includes paint shops, gasoline storage or loading areas, and other sources of dust, dirt, and corrosive, toxic, or inflammable gases.

14

Don't put exterior glass walls and windows in vulnerable locations.

Although the number is steadily decreasing, a fairly large number of data processing centers are still located behind glass walls or large glass windows on ground floors. These are readily visible and available from sidewalks or highways. Centers which are exposed in this manner risk possible destructive tactics on the part of dissident groups or individuals.

In many locations, the threat isn't severe enough to justify bricking up the windows or moving the location. Consider using venetian blinds or similar covering inside the windows. One of the better grade plastic materials is recommended as replacement or exterior cover for the present glass. Clear plastic glass-substitutes will do a good job of deflecting thrown stones or incendiary materials, and their cost is sufficiently low to make their installation economically feasible in most centers.

15

Have instructions and procedures on what to do in the event of fire or fire alarms.

Personnel expected to use fire extinguishers should be trained in their use. They should receive some classroom instruction in the mechanics of fire-fighting and then be taught to operate hand-held extinguishers. This should be followed by allowing them to practice putting out a fire in the parking lot or other suitable area.

If there are fire detection systems which will activate fire-quenching systems unless there is human intervention during some fixed delay, all operating personnel should be taught how to use them. Conversely, it's important that all personnel be told not to intervene automatically and prevent actuation of the quenching system, unless they are certain that there is no fire.

16

Protect your system against smoke damage.

Smoke, particularly the kind that is primarily heavy, black, particulate matter, can be very damaging and requires a lengthy and costly clean-up operation. Most smoke reaching into and damaging data processing systems originates from fires external to the data processing center. It is frequently pulled into the center through the air-conditioning system.

You should examine your potential for this problem and take appropriate measures to operate dampers to stop the intake of smoke. Similarly, fitted plastic covers for all of the equipment, desks and storage cabinets can help to reduce smoke damage. They are inexpensive and easily made. They can be stored in relatively small spaces. Label them appropriately and prominently, identifying which units they fit, to make it easy to install them on short notice and under conditions of relatively high stress.

Getting smoke out of your system area fast can be done by using separate exhaust fans. These are useful after a limited but smoky fire has been extinguished.

17

Protect your system against water damage.

Water damage can occur as a result of leaking rooftop cooling towers, leaking roofs—even on new buildings—leaking pipes in the overhead, and the operation of sprinkler systems on floors above the data processing center. Protect the equipment and associated furniture and cabinets against water and devise a plan for rapidly removing any water that may enter the area. Pay particular attention to installing drains under the raised floor where the system cables are installed. The fitted plastic covers mentioned in the preceding paragraph on smoke are invaluable in protecting the equipment against water coming through the ceiling.

18

Maintain good working relations with the local fire department.

Get acquainted with the local fire department before they are called in an emergency. Make the department aware of the particular vulnerabilities of the system to extensive quantities of water coming through the overhead and the desirability of venting smoke so as to minimize the amount reaching the data processing area. It is not reasonable to anticipate that the fire department will be fully aware of the peculiar situation presented by your particular installation. They won't extend appropriate concern for the safety of the data processing system if you haven't given them an opportunity to review it. Further, they can usually offer excellent advice as to precautions which should be taken to prevent fire.

19

Maintain a good working relationship with local police departments.

DP center management and the plant or facilities security personnel and a corporate attorney should meet with senior representatives of the local police departments. Be sure you know the appropriate police department to be called in the event of emergencies. It is not uncommon for a facility to be serviced by as many as three or four separate police departments. Their response times may vary widely between day and night, so that it may be appropriate to call one during the day and another at night.

In deciding which police department to call, it is also important to determine what they will do for you. It is commonly, often erroneously, believed that the police can be called to remove any trepassers from the property. They frequently will not do this except under specific circumstances. These circumstances must be understood so that the persons responsible for calling the police will know what particular service the police can be expected to provide.

20

Dont rely too much on guards or a small guard force for protection against civil disturbances.

The value of a single unarmed guard at the door as a deterrent against reasonably determined dissident groups bent on damaging or destroying a facility is commonly overestimated. Similarly, the protection afforded by locked doors, particularly if they delay entry for even a few minutes, is often underestimated. It would be appropriate for you to compare the cost of a fully effective guard force and the cost of a back-up facility that will provide a limp-along capability if the principal facility is lost through a civil disturbance.

21

Take into account any specialized requirements of your data processing center when you establish procedures and instructions for responding to bomb threats.

Most large organizations, particularly those which have had bomb threats, have developed a more or less standard response to such threats. But they haven't always considered the peculiar requirements of the data processing center under such circumstances. Whenever the after-hours telephone number of the data processing center has been widely publicized, for example, the number of bomb threats made directly to the center appears to increase. This is particularly true when the center is a separate building.

If the established response to a bomb threat is to evacuate the entire facility, then you should consider securing the DP center from intrusion by those who might remain in the building. Unless this is done, it is quite possible for persons in the building to initiate a bomb threat, cause evacuation of the personnel from the DP center, and then be free to enter the computing area and damage it. In addition, the more valuable files, particularly those including transaction logs, should be identified as part of a bomb threat response plan, so that they can be properly protected or backed up, if an explosion actually occurs.

22

Assess the need for protection against power failures or voltage reductions.

Frequently, when an organization decides it needs backup electrical generating capacity or uninterrupted power systems, the choices are often made without an adequate knowledge of the external environment which creates the problem. Almost as frequently, there is no full understanding of the internal environment which requires that this problem be solved.

Many kinds of equipment are available to provide protection against power line disturbances, power line transients and long-term voltage reductions. You should fully understand the particular needs of each DP center, including anticipated growth in power requirements, if you are going to come up with operationally suitable and economically satisfactory solutions to these problems.

23

Have a realistic understanding of how magnets can damage magnetic storage media.

Both the general press and the trade press have given widespread and often grossly exaggerated coverage to instances in which magnetic storage media in a data processing center or tape libraries were reported to have been damaged by magnets. The management of some DP centers has overreacted to the potential damage magnets can do to storage media, while the management of other centers has ignored the problem altogether. The appropriate course lies somewhere between these two extremes.

Magnets brought sufficiently close to magnetic storage media can seriously damage or erase the information recorded there. Even a very small magnet brought into direct physical contact with magnetic tape or disk or drum surfaces can destroy recorded data. But the ability of any magnet to erase data decreases very rapidly with distance.

As a consequence, even very large magnets cannot damage data at distances in excess of a few inches—say 20 inches to be safe. Except in unusual circumstances, distances of six to eight inches between the media and even very large magnets would provide adequate protection for the recording medium. Thus, such things as magnetic cabinet latches in the macine room have the potential for damaging tapes which are brought in immediate physical contact with them. For this reason, they should not be used in the machine room.

If flashlights with magnets for holding them against metal surfaces must be brought into the DP center, great care should be exercised in their control. In general, don't use them in the machine room.

24

Set up procedures to control portable transceivers.

Small portable radio receivers are used by many people to receive calls or signals that they should call their offices. These receivers will not disrupt data processing equipment. However, some portable transceivers, which provide the capability for transmitting back to the caller, do have a potential for disrupting data processing equipment if they are operated in the same room or very close to the computing area. Areas immediately above or below the center are as vulnerable as areas on the same floor. Radio transmitters should either be excluded from the machine room or tested to see that they don't interfere with the operation of the system.

Most modern computing systems are designed to withstand electromagentic fields generated by local radio stations and radars. However, even low-power transmitters that are very close to the equipment may generate quite high field strengths within these units with the potential for causing some disruption. Tests of these devices for their ability to disrupt are not difficult, but unless your DP center management is aware of their potential for disrupting system operation, numerous interruptions can occur which might otherwise be unexplained.

25

Limit access to terminals.

Terminals that are left unprotected can be misused. Any terminals which can be used to access system-managed data should be locked in a secure area or equipped with key-operated power-on switches so that they cannot be used except by those who have the proper keys. Similarly, you should consider the best way to identify terminal operators to the system. A record within the system of who specifically conducted what transaction, read what data, or modified which file is generally a powerful deterrent to misuse. (There's a related discussion of audit trails in Number 41.)

26

Change keys, combinations and passwords frequently.

Unless keys, combinations and passwords are changed with reasonable frequency, once they are compromised, they are compromised for significant periods of time. Further, reasonably frequent changes of such items reaffirms to all personnel management's continuing concern for security.

27

Limit access to your working tape and disk libraries.

It is still quite common to see that many people have virtually uncontested access to working tape and disk libraries. It is also fairly common to see concrete block walls around a tape library. The walls have been provided to restrict access to the room, but they have doors that stand open virtually all of the time.

These walls often do more to invite damage to the tapes than they do to protect them. They make the area hard to supervise from outside and make it possible for an intruder to do considerable damage before being noticed. Whenever access to the entire area is adequately controlled, waist-high partitions or glass walls may offer greater security than vault-like walls on these libraries.

In short, procedures should be introduced to assure proper authorization of all withdrawals from the libraries. This assures you that access is limited to only those people who must have access, helps account for all material removed from the library, and helps protect files against fire, water, smoke, and damage by disgruntled employees.

28

Maintain adequate backup files.

Relatively elaborate plans for the preparation and storage of backup files are more common than are really workable plans that are fully, or even partially, implemented. Any plans for backup files should be reviewed periodically for adequacy, and to make sure that they have, in fact, been implemented.

29

Test your backup files.

It is highly desirable that a complete rundown of the recovery procedures involving backup files be written and then carried out. There is some probability that untested backup files may be unusable.

30

Plan for and test backup data processing facilities.

Contingency plans involving the use of backup data processing facilities if the primary facility is damaged or destroyed are incomplete until the backup facility has been tested. Again, a complete procedure involving all activities, from the loss of the primary facility to recovery on the backup facility, should be written and carried out including actual processing of backup files on the backup facility. Incompatibility because of configuration differences or feature mismatches is so probable that such tests should be conducted if there is any chance you may have to depend on the availability of a backup facility.

31

Identify or prioritize critical operations in planning for backup facilities and other recovery activities.

Recovery from disasters or major disruptions almost always implies a period of limp-along or degraded operations. It is important that the temporarily limited data processing capability be expended on the most critical activities—which is possible only if they have been properly identified.

32

Set up procedures for delivering records to archival storage and recovering them.

Care should be taken to properly identify representatives of the delivery service who transport materials to and from archival storage. It is sometimes too easy to simply appear at about the appointed time and indicate that you are from the agency which delivers records to storage and be given all of the materials ready for transport. These materials are normally quite rich in information because they have been specially selected as the most valuable records. Thus, the inducement to pose as the deliveryman is reasonably high.

33

Control the use of information on scratch packs or tapes and other residual data.

Information can be disclosed to unauthorized persons when it's left on scratch packs or tapes that these persons can use. Care should be taken to clear the secondary storage media of sensitive data or to deny their use to those who might misuse the residual data to them.

Another example: it is not uncommon to see persons from payroll, or accounting, or elsewhere, erect screens around a printer on which sensitive data such as financial status information for quarterly or annual reports or payroll or cash position is being printed. Then, when the printing is completed, they take the output and go happily away feeling quite secure. Meanwhile, they've left all of the same information on tape or packs in the machine room and available to

anyone with access to the system and enough curiosity to generate another printed output.

34

Keep your operating areas clean and neat.

All of the reasons for having neat, clean operating areas are too numerous to list here. However, some of the problems you can avoid are: the fire hazard generated by the accumulation of paper under the raised floor; the potential damage to equipment from spilling coffee, milk or hot chocolate into system components; the ease with which one or two tapes or packs can be removed from the area if large numbers of them are allowed to accumulate; the fire hazard presented by storing excessive paper supplies; the fire hazards caused by smoking; and the false alarms created in smoke detection systems. These are just a few problems encountered in operating areas with sloppy housekeeping rules.

35

Set up security-minded procedures for receiving and storing paper supplies.

Your receiving platform often gives the potential intruder ready access to the entire facility or an opportunity to deliver incendiary materials that would destroy the facility. Care should be taken to limit the use of the receiving platform as a means of entering the building.

Further, paper supplies, other than those needed to satisfy the immediate requirements of the data processing center, should be stored in a location properly designed to provide adequate fire detection and fire-quenching facilities. Excessive quantities of paper materials stored in and about the equipment areas constitute a significant, and unnecessary, fire hazard.

36

Keep sensitive data out of the outgoing paper trash.

The paper material on the loading platform waiting for the trash man can be a highly rewarding source of sensitive information for those who would beat the trash man to it or buy it from the trash man later. Sensitive data should be shredded as part of your disposal procedure. As a minimum, boxes of cards should be dumped so that extreme efforts would be required to put them back in the proper groups and sequences. Particular care must be paid that interpreted cards be indecipherable.

37

Set up thorough procedures to protect programs, run instructions, object decks, etc.

Care given to the acquisition and storage of data can be wasted unless adequate attention is given to the appropriate protection of programs. Programmers often have such a strong feeling of ownership about their own programs that they store them in their offices, often inadequately protected there, and not generally available for archival storage—at least in their most recent version. Programs, instructions for their use, object decks and similar materials should be given the same protection extended to the data. Programs, like data, are a valuable corporate asset and are entitled to protection as such.

38

Tighten up procedures for controlling your application programs.

In addition to protecting application programs as assets, it is also often necessary to establish stringent controls over modifications to the programs to make certain that the changes do not cause accidental or intentional damage to the data or its unauthorized disclosure.

Limitations on the scope of application programs, insistence on initial objectives and specifications, audit and test, review of modifications, exclusion when necessary of application programmers from system areas, and effective constraints on the use of application programs by the programmers who wrote them must all be considered as valid security measures for protecting data in the system. Particular attention must be given to the potential of the disgruntled programmer employee to do extensive damage through unauthorized program modification.

39

Set up procedures to control the use of paper output.

Keeping track of multiple copies, indicating confidentiality or "for internal use only," and using page numbers such as "page 1 of 9 pages," should all be considered as ways to control the distribution and possible diversion of copies of printed output.

Unfortunately, it's common to see large volumes of sensitive information lying around in offices and relatively available to large numbers of people. It is difficult to justify extensive security measures in the data processing center if adequate controls aren't extended to the paper output from the system.

40

Establish procedures and instructions for system operators.

One person whose disloyalty, poor judgment, or incompetence is most difficult to protect yourself against is the system operator. Special attention should be given to determining his loyalty, to defining the latitude which he is given to innovate and modify established operational procedures and run instructions for programs, and to the possibility of more firmly enforcing a two-operator rule.

41

Use audit trails or transaction logs as security measures.

An audit trail or complete transaction log can be a very effective security measure. It is very difficult to build a system in which the necessary security is achieved by making the system too difficult to penetrate.

The more economical way of achieving security is to make the system reasonably difficult to get into and then provide a significant deterrent by threatening to detect any successful penetrations. Such detection would then result in disciplinary action. As an analogy, even very secure buildings often require guards inside in the event the barriers to penetration are not always successful.

It is highly desirable that the system be used to process the transaction log to look for potential security violations. In many instances, it is not completely feasible to pull out the transaction log and examine it manually. Failure to provide a processor for the transaction log may wholly defeat its use as a security measure.

42

Test physical security measures and operating procedures to see if they are effective.

Failure to test security measures can easily result in reliance on a number of things which are ineffective. It may also imply to all personnel affected by them that there is little management interest in security. Thus, reasonably frequent tests of security measures indicate a continuing awareness and concern for security. For that reason, they are themselves a security measure. They improve the sensitivity of employees toward security as a continuing problem.

Chapter 8. Standards and Documentation

IBM SYSTEM/32 SUPPORT MANUALS

Contact your IBM Sales Representative for the manuals required at your account.

Required	Title	Form Number
_____	*Introduction*	GC21-7582
_____	*Installation and Physical Planning*	GA21-9177
_____	*Messages Glossary*	GC21-7641
_____	*Functions Reference Manual*	GA21-9176
_____	*Control Program Reference Manual*	GC21-7593
_____	*Operator's Guide*	GC21-7591
_____	*Program Product Reference—DFU*	SC21-7600
_____	*Program Product Reference—SEU*	SC21-7605
_____	*Utilties Program Product Reference—SORT*	SC21-7633
_____	*RPG II Reference*	SC21-7595
_____	*System Messages Guide*	GC21-7592
_____	*System Messages Guide—RPG II*	SC21-7617
_____	*Utilities Program Product Messages Guide*	SC21-7618

Other Manuals

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

IBM System/3 Support Manuals

(Check System Bibliography, GC20-8080)

READER'S COMMENT FORM

G360-0011-0

Installation Guide
System/32, System/3

Please comment on the usefulness and readability of this publication, suggest additions and deletions, and list specific errors and omissions (give page numbers). All comments and suggestions become the property of IBM. If you wish a reply, be sure to include your name and address.

COMMENTS

fold fold

fold fold

- Thank you for your cooperation. No postage necessary if mailed in the U.S.A. FOLD ON TWO LINES, STAPLE AND MAIL.

Your comments, please . . .

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. Your comments on the other side of this form will be carefully reviewed by the persons responsible for writing and publishing this material. All comments and suggestions become the property of IBM.

Fold Fold

First Class
Permit 9314
Atlanta
Georgia

Business Reply Mail

No postage stamp necessary if mailed in the U.S.A.

Postage will be paid by:

International Business Machines Corporation
Technical Communications, Dept. 805
P.O. Box 2150
Atlanta, Georgia 30301

Fold Fold

IBM®

International Business Machines Corporation

General Systems Division
5775D Glenridge Drive N.E.
P.O. Box 2150
Atlanta, Georgia 30301
(U.S.A. only)

General Business Group/International
44 South Broadway
White Plains, New York 10601
U.S.A.
(International)

International Business Machines Corporation

General Systems Division
5775D Glenridge Drive N. E.
P.O. Box 2150
Atlanta, Georgia 30301
(U.S.A. only)

General Business Group/International
44 South Broadway
White Plains, New York 10601
U.S.A.
(International)

Installation Guide—System/32, System/3 Printed in U.S.A. G360-0011-0

G360-0011-0