CA MICS® Resource Management

Standard Reports Guide

Release 12.9

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: INTRODUCTION

The CA MICS Standard Reports Guide is the primary reference for those individuals requiring information on the standard Exception Reports produced by CA MICS. The remaining chapters of this manual cover the following topics:

Chapter 2, Exception Reports, itemizes the individual exceptions, describes the reporting process, and explains the method by which users may adjust the threshold values used in the exception detection process.

If you have any questions about the definition, operation, or interpretation of the standard reports for which you cannot find answers in this manual, please contact CA Technical Support.

Note: For information about the standard reports available by product and options for modifying report parameters, refer to the individual product guides.

Other documentation available with CA MICS includes:

```
**************************
* GUIDES FOR THE END-USER *
**************************

CA MICS Database Structure and Content Guide
CA MICS Document Access Guide
CA MICS MICF Reference Guide
CA MICS MICF User Guide

**************************************
* GUIDES FOR THE SYSTEM ADMINISTRATOR *
**************************************

CA MICS How to Use the PSP
CA MICS Planning, Installation, Operation, and Maintenance
   Guide (PIOM)
CA MICS Standard Reports Guide
CA MICS System Administrator Guide
CA MICS System Modification Guide
```

```
******************
* PRODUCT GUIDES *
******************

CA MICS Accounting and Chargeback Option Concepts and
   Overview Guide
CA MICS Accounting and Chargeback Option User Guide
CA MICS Analyzer for TSO Guide
CA MICS Analyzer Option for CA IDMS Guide
CA MICS Analyzer Option for CICS Guide
CA MICS Analyzer Option for DB2 Guide

CA MICS Analyzer Option for IMS Guide
CA MICS Analyzer Option for MeasureWare Guide
CA MICS Analyzer Option for MQSeries Guide
CA MICS Analyzer Option for VAX/VMS Guide
CA MICS Analyzer Option for VM/CMS Guide
CA MICS Analyzer Option for VSE/Power Guide
CA MICS Batch and Operations Analyzer Guide
CA MICS CA ASTEX Option Guide

CA MICS Capacity Planner Option Guide
CA MICS Data Transfer Option for VM/CMS Guide
CA MICS Hardware and SCP Analyzer Guide
CA MICS IMS Log Data Extractor Option Guide
CA MICS Network Analyzer Option Guide
CA MICS Performance Manager Option Guide

CA MICS Space Analyzer Option Guide
CA MICS Space Collector Option Guide
CA MICS StorageMate Option Guide
CA MICS System Reliability Analyzer Option Guide
CA MICS Tandem Option Guide
CA MICS Tape Analyzer Option Guide
CA MICS Web Analyzer Option Guide
```

Chapter 2: EXCEPTION REPORTS

The exception process provides management and technical personnel with a means to specifically identify problems or problem areas, organize and report the problems in terms of their severity, integrate the problem reporting for all system components, and associate the problems to their respective management areas.

This process is called Exception Reporting and operates daily to process the updated database and report each day's exceptions.

Figure 2-1 depicts the inputs, operational flow, and outputs related to this daily process.

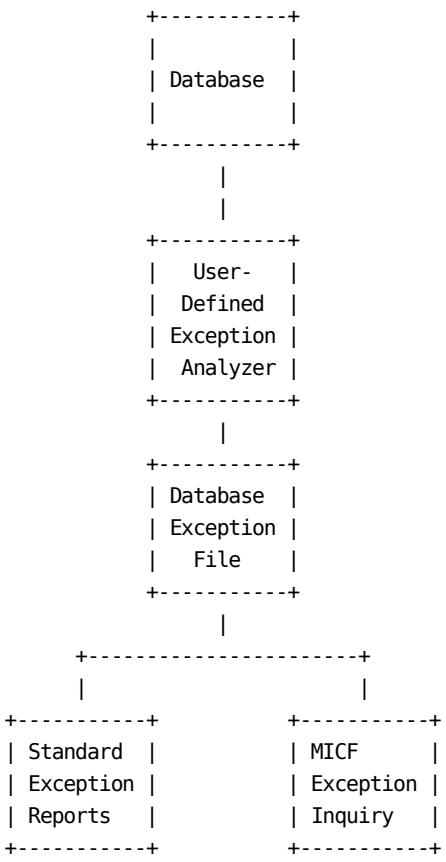


Figure 2-1. Exception Reporting Operational Flow

On a daily basis the appropriate files contained in the database are processed to detect the defined exception conditions. The Exception Analyzer performs this task by using individual test routines to identify the exceptions. Each test routine requires the necessary user-defined values which tailor the exception test to the installation requirements.

The test routines are provided with each distributed component (e.g., TSO test routines, RMF test routines, etc.). These tests are called Exception Test Routines (ETRs) and are stored in their respective unit source library (e.g., sharedprefix.MICS.SOURCE) in the member DYcccEXC, where ccc represents the applicable component identifier, such as SNT for the SNA Network Analyzer.

Each exception test may be identified within the source module named above by its assigned exception number. The text condition and definition is written in SAS and consequently may be easily modified by the user. The exception test condition also sets the exception number, defines the severity, assigns the exception to a management area, defines the appropriate text message to explain the exception, and establishes the necessary tests to identify the exception condition.

Standard reports and online inquiries are available in reporting the exception information. The standard reports include an Exception Management Overview, the Severity Level Exception Summary, and optionally, the Management Area Exception Summary. Online inquiry provides the user with the ability to produce the Exception Full Detail Report which itemizes the detected exceptions on an individual basis. The online inquiry facility enables the user to quickly retrieve the Exception Full Detail report online by specific selections on exception number, severity level, management area, user, and standard date and time.

This reporting structure is used with the emphasis being on first providing management a concise summary of the frequency of problems in the Exception Management Overview. An integrated, time-of-day oriented report provides the performance analyst and systems team with a summary of which exceptions, ordered by their severity, have been detected over the hours of the day. Based on the exceptions reported and the known problems, the performance analyst can then employ the online inquiry to analyze quickly, and in-depth, the detail exceptions and the database information from which they were taken, to complete the research and resolution of the reported items.

The Exception Reports provide a concise, integrated, and itemized list of the problems impacting an installation's effectiveness in terms of availability, service, workload, standards, security, and performance for the different areas of responsibility (e.g., TSO, Batch, MVS).

This chapter contains sections to describe the philosophy and requirement of exception reporting, a general description of the process, the methodology for qualifying exceptions, an explanation of the operational flow, a list of the exceptions provided, a description of the reports, a plan for the use of the reports, and the more detailed descriptions required to explain the exception definition process.

This section contains the following topics:

2.1 The Exception Reporting Process

The technique of exception reporting has always had value for data processing management. The increase in growth and complexity, however, make exception reporting a necessity in even the smallest z/OS data centers. The problem is that a given CPU processor or processor complex of CPUs operates using numerous components (e.g., SCP, TSO, JES2, Batch, VTAM), each of which are performing a significant level of processing. This combination of functions, which generally processes larger and more diverse workloads, results in an increase in complexity and load making the management control problem difficult, if not impossible.

It is because of this increased complexity and activity that an exception reporting process should be used as a diagnostic filter to report specific problems or potential problem areas. The concept of exception reporting operates like an automated medical system for diagnosing the presence or probability of heart failure. By processing the monitored responses of the patient and matching them against previous patterns of heart sickness and certain definable thresholds for blood pressure, pulse rate, etc., it is possible to provide a diagnosis of the possible problems.

The Exception Reporting system described in this chapter operates like a medical diagnosis system, by inputting available monitoring sources (e.g., RMF, CA TSO/MON PM, SMF), comparing this activity against pre-defined thresholds, and providing an integrated exception list of potential problem areas.

Exception Reporting is designed to reduce the number and volume of reports that the systems programmer, performance analyst, security officer, and so on has to wade through for analysis. Furthermore, by reporting the exceptions from the different components in an integrated manner, the time spent in problem tracking should be reduced while at the same time increasing the effectiveness of the systems and performance teams through a more controlled, systematic reporting of the exceptional conditions impacting the installation's operation.

IDENTIFYING AND QUALIFYING EXCEPTIONS

The identification and qualification of the exceptions to be reported is essential to an effective and usable exception reporting process.

The identification of which exceptions should be reported is addressed in large part by the exceptions which are distributed as a standard part of CA MICS. The concept of exception analysis is to identify and report only those occurrences which merit visibility and attention. Exception reporting may be used to report an occurrence that is a distinct problem (e.g., TCAM/VTAM outage at 2:00 pm), one that may be a problem (e.g., TSO user overloaded the system from 1:00 to 1:30 pm) and requires further research, or represents a standard, security, or audit violation (e.g., user XYZ is not authorized to use SUPERZAP and was detected using it seven times last week).

The user may tailor the standard exceptions as explained in this chapter (in the section on Exception Values).

It is one thing to define exceptions, but quite another problem to organize and report them in a usable manner. Most individuals would expect that simply identifying the exceptions finishes the job. The anomaly one will encounter is that the exceptions themselves will probably be quite voluminous and they too, require categorization, aggregation, consolidation, and prioritization. This is what is meant by exception qualification.

The Exception Reporting process enables an exception to be qualified, and thereby reported, in the following ways:

- o Exception Number for unique definition

  Exception numbers uniquely identify individual exceptions. The numbers are sequentially assigned within the sharedprefix.MICS.SOURCE(DYcccEXC) members.

- o Severity Level to signify degree of importance
  A severity level code is assigned to each exception in order to differentiate the importance of different exception types. The definition of severity level allows for three categories: critical, impacting, and warning. The assignment of severity level is, of course, subjective. The following guidelines are suggested for this purpose.

- o Critical: Assigned to an exception that represents a missed service guarantee (e.g., availability, response, turnaround), a missed management objective (e.g., maximum of 5 IPLs per month), a security violation, or a serious violation of an installation standard or audit guideline.

- o Impacting: Assigned to an exception that represents performance degradation related to reliability, service, capacity, turnaround, etc., which has created a political situation, or has in any way manifested itself in a noticeable problem short of the critical definition.

o Warning: Assigned to an exception that represents a preventative maintenance problem (e.g., buffers are running low), a symptomatic performance problem (e.g., demand paging rate is above normal), or a general installation standard or audit guideline that was violated.

The assignment of the severity level enables the exception reports to be prioritized by the level of seriousness of the reported problems, as well as provide a method for exception report selection.

o Management Area to identify area of responsibility
A management area code is assigned to each exception enabling the exception to be associated to the area of responsibility (e.g., Availability).
The management area code is used primarily for reporting purposes and provides a means to organize the exceptions.

The following list depicts the management areas defined and in use:

o Availability: Computing hardware (e.g., CPU) or software subsystems (e.g., TSO) reliability and availability.

o Performance: Computing hardware, operations, supervisory software, or program product performance.

o Productivity: Operational and development personnel productivity.

o Security: Physical access, system integrity, and data access security.

o Service: Online response times and batch turnarounds.

o Standards: Enforcement of installation defined standards, guidelines, and policies.

o Workload: User submitted load in terms of system effectiveness, performance, and operation.

The management area assignment then enables the exceptions to be analyzed by Information Areas (e.g., TSO, Hardware Utilization) or Information Area within management area.

2.2 Report Descriptions

Exception Reports provide a concise, integrated method for problem reporting. This section describes the standard and online inquiry reports.

The three standard reports produced daily are:

o Exception Management Overview

o Severity Level Exception Summary

o Management Area Exception Summary

The online inquiry facility described in Chapter 5 of the MICF Reference Guide enables you to produce two exception detail reports:

o Full Exception Detail

o Short Exception Detail

Exception reports are not changed in number or format with the inclusion of additional Information Areas. The only difference is that the new Information Area adds another set of exceptions which are reported by this integrated process.

The following sections describe the format, options, and use of the five exception reports:

1 - Exception Management Overview
2 - Severity Level Exception Summary
3 - Management Area Exception Summary
4 - Full Exception Detail
5 - Short Exception Detail

2.2.1 Exception Management Overview

This report provides a concise, high-level summary of the exceptions that have been reported. The report is structured to report the number of exceptions in terms of their severity for each of the defined management areas.

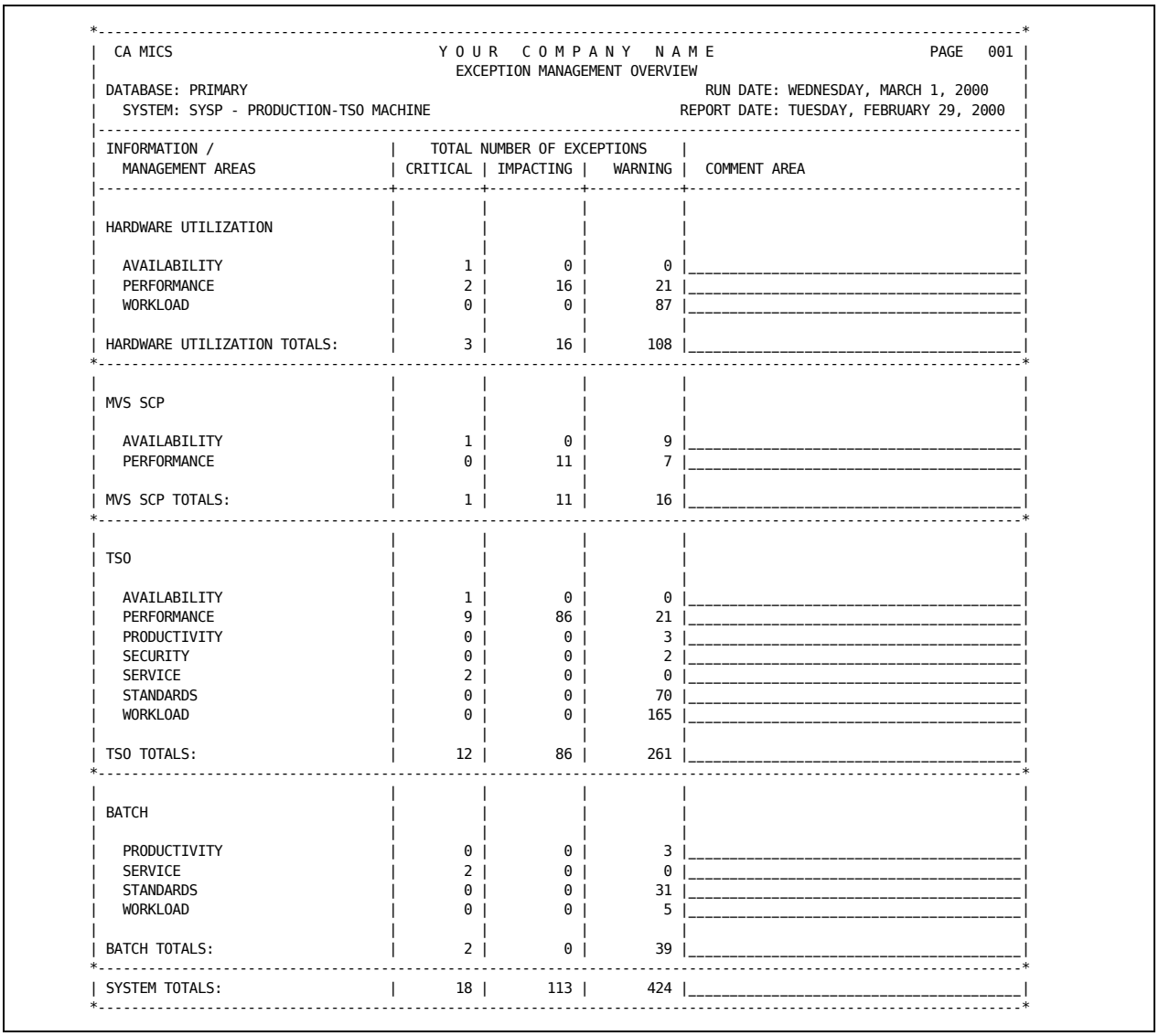
The purpose of the report is to provide upper-management with a distribution, in terms of severity and area of responsibility, of the problems impacting the installation. From upper-management's perspective as long as there were few, or no, critical problems reported, or there is not a marked increase in the number of problems in any management area, then the report provides a quick assessment that the operation is at least stable.

This report is produced as the first output in a daily exception reporting process for each computing system contained in the database.

Figure 2-2 illustrates the one-page format of this report. The report heading gives the name of the report, system and unit database being reported on, Run Date, and Report Date in addition to identifying this as a CA MICS report and displaying your company name.

The body of the report identifies the management areas (e.g., STANDARDS) within each of the active Information Areas (e.g., TSO, MVS SCP). The reporting is by management area and quantifies in the next three columns the number of critical, impacting, and warning exceptions that have been identified for each management area. A comment area is provided to facilitate the user's ability to enter commentary or reference notes on the report.

The last line of the report provides a total of all exceptions by their severity levels.



CA MICS Y O U R C O M P A N Y N A M E PAGE 001
EXCEPTION MANAGEMENT OVERVIEW
DATABASE: PRIMARY RUN DATE: WEDNESDAY, MARCH 1, 2000
SYSTEM: SYSP - PRODUCTION-TSO MACHINE REPORT DATE: TUESDAY, FEBRUARY 29, 2000

INFORMATION / MANAGEMENT AREAS	TOTAL NUMBER OF EXCEPTIONS CRITICAL	IMPACTING	WARNING	COMMENT AREA
HARDWARE UTILIZATION				
AVAILABILITY	1	0	0	
PERFORMANCE	2	16	21	
WORKLOAD	0	0	87	
HARDWARE UTILIZATION TOTALS:	3	16	108	
MVS SCP				
AVAILABILITY	1	0	9	
PERFORMANCE	0	11	7	
MVS SCP TOTALS:	1	11	16	
TSO				
AVAILABILITY	1	0	0	
PERFORMANCE	9	86	21	
PRODUCTIVITY	0	0	3	
SECURITY	0	0	2	
SERVICE	2	0	0	
STANDARDS	0	0	70	
WORKLOAD	0	0	165	
TSO TOTALS:	12	86	261	
BATCH				
PRODUCTIVITY	0	0	3	
SERVICE	2	0	0	
STANDARDS	0	0	31	
WORKLOAD	0	0	5	
BATCH TOTALS:	2	0	39	
SYSTEM TOTALS:	18	113	424	

Figure 2-2. Exception Management Overview Report Sample

2.2.2 Severity Level Exception Summary

This report provides a concise hourly summary of the exceptions that have been encountered. The report is structured to report the exception types, and the number of times they have been detected, for each hour of the day, with the report organized to display the critical exceptions first, then the impacting, and finally the warning exceptions.

The purpose of the report is to provide first-level management, performance analysts, and systems programmers with an integrated report of the different problems that may have impacted the installation in any given hour. The first objective is the specific identification of a problem (e.g., exhausted the TSO TIOC buffers). Secondly, however, the method is attempting to illustrate the relationship that may exist between different system components by reporting the different exceptions in an integrated manner. For instance, the report may specify that a TSO response objective was missed as a critical exception. For the same hour, however, it was also reported that a vital channel was taken offline, which also constituted a critical exception for the same hour. Knowing that these two situations have happened during the same hour the performance analyst has a potential resolution for the response problem.

The objective is to provide a quick assessment of the different types of exceptions that have been detected throughout a day, without requiring the report user to reference through the full listing of individual exceptions.

Figure 2-3 illustrates the format of this report. The heading shows the report title, system and unit database being reported on, date the report was run, and the time period being reported on (Report Date) as well as the usual company and product identification.

At the start of each new severity level to be reported, a subtitle box is printed at the top of a new page to specify the severity level being reported.

The body of the report identifies the calendar date and hour within which the reported exception occurred, the count of the number of times that the exception was detected within the hour, the exception number identifying the exception, the message text describing the exception, and finally in the last column the management area to which this exception has been assigned.

The report is produced in three sections, with each section starting on a new page. The first section reports all critical exceptions, the second the impacting exceptions, and the third the warning exceptions.

```
CA MICS                                  Y O U R   C O M P A N Y   N A M E                                  PAGE 0001
                                          SEVERITY LEVEL EXCEPTION SUMMARY
DATABASE: PRIMARY                                                                  RUN DATE: WEDNESDAY, MARCH 1, 2000
  SYSTEM: SYSP - PRODUCTION-TSO MACHINE                                  REPORT DATE: TUESDAY, FEBRUARY 29, 2000

                                        SEVERITY LEVEL: CRITICAL

           HOUR |     E X C E P T I O N                                                          |  MANAGEMENT|
   DATE   OF DAY|   COUNT NUMBER  DESCRIPTION                                                    |    AREA    |
----------------+--------------------------------------------------------------------------------+------------|
 29FEB00   9:00 |                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                         |            |
                |                                                                                |            |
          10:00 |                                                                                |            |
                |       6 00101 - CRITICAL TSO TIOC BUFFER LEVEL DETECTED                        |PERFORMANCE |
                |       1 00203 - HOURLY TSO SHORT SERVICE OBJECTIVE MISSED                      |SERVICE     |
                |       1 00208 - TCAM/VTAM OUTAGE DETECTED                                      |AVAILABILITY|
          11:00 |                                                                                |            |
                |       2 00100 - SYSTEM IPL DETECTED                                            |AVAILABILITY|
                |       1 00203 - HOURLY TSO SHORT SERVICE OBJECTIVE MISSED                      |SERVICE     |
                |       1 00206 - HOURLY TOTAL TSO SERVICE OBJECTIVE MISSED                      |SERVICE     |
                |       1 00207 - HOURLY TSO AVAILABILITY OBJECTIVE MISSED                       |AVAILABILITY|
                |       2 01000 - SYSTEM ID INCORRECT FOR HARDWARE SERIAL NUMBER                  |STANDARDS   |
                |       2 02008 - AUXILIARY STORAGE SWAP OCCURRED                                |PERFORMANCE |
                |       1 02015 - INSUFFICIENT PAGEABLE FRAMES                                   |PERFORMANCE |
          12:00 |                                                                                |            |
                |       2 00100 - SYSTEM IPL DETECTED                                            |AVAILABILITY|
                |       1 00203 - HOURLY TSO SHORT SERVICE OBJECTIVE MISSED                      |SERVICE     |
                |       1 00206 - HOURLY TOTAL TSO SERVICE OBJECTIVE MISSED                      |SERVICE     |
                |       1 00207 - HOURLY TSO AVAILABILITY OBJECTIVE MISSED                       |AVAILABILITY|
          13:00 |                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                         |            |
                |                                                                                |            |
          14:00 |                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                         |            |
                |                                                                                |            |
          15:00 |                                                                                |            |
                |       1 02500 - UNUSABLE PAGE SLOT OR SWAP SET DETECTED                        |PERFORMANCE |
          16:00 |                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                         |            |
                |                                                                                |            |
          17:00 |                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                         |            |
                |                                                                                |            |
```

Figure 2-3. Severity Level Exception Summary Report Sample

2.2.3 Management Area Exception Summary

This report provides a concise hourly summary of the exceptions that have been encountered. The report is structured identically to the Severity Level Exception Summary described in the previous section. The difference is in the sequenced organization. Where the other report organized and separated the exceptions by severity level, this report organizes and reports the exceptions by management area, in the following order:

- Availability
- Performance
- Productivity
- Security
- Service
- Standards
- Workload

The purpose of the report is to provide first-level management having the responsibility for one or more of the above areas with a concise list of those exceptions pertinent to their area of responsibility. The report is probably required in larger installations where there are numerous departments involved with operating the installation. This report would be considered optional for the small-to-medium scale installation.

Figure 2-4 illustrates the format of this report. The heading shows the report title, system and unit database being reported on, date the report was run, and the time period being reported on (Report Date) as well as the name of the company and product identification.

At the start of each new management area a subtitle box is printed at the top of a new page to specify the management area being reported. The report is produced with a section for each management area reported, with each section starting on a new page.

```
-------------------------------------------------------------------------------------------------------------------------------*
 CA MICS                                  Y O U R   C O M P A N Y   N A M E                                    PAGE 001   |
                                           MANAGEMENT AREA EXCEPTION SUMMARY                                              |
DATABASE: PRIMARY                                                                    RUN DATE: WEDNESDAY, MARCH 1, 2000    |
  SYSTEM: SYSP - PRODUCTION-TSO MACHINE                                            REPORT DATE: TUESDAY, FEBRUARY 29, 2000  |
-------------------------------------------------------------------------------------------------------------------------------|
                                              MANAGEMENT AREA: WORKLOAD                                                        |
-------------------------------------------------------------------------------------------------------------------------------|
           HOUR |     E X C E P T I O N                                                                          | SEVERITY   |
   DATE   OF DAY|   COUNT NUMBER  DESCRIPTION                                                                    |  LEVEL     |
----------------+--------------------------------------------------------------------------------------------------+------------|
 29FEB00   9:00 |                                                                                                |            |
                |       2 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
          10:00 |                                                                                                |            |
                |       7 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
          11:00 |                                                                                                |            |
                |         ***** - NO EXCEPTIONS REPORTED                                                         |WARNING     |
          12:00 |                                                                                                |            |
                |       2 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
          13:00 |                                                                                                |            |
                |      15 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
          14:00 |                                                                                                |            |
                |       6 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
                |       1 00002 - INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                              |WARNING     |
          15:00 |                                                                                                |            |
                |      10 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
                |       1 00002 - INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                              |WARNING     |
          16:00 |                                                                                                |            |
                |       4 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
          17:00 |                                                                                                |            |
                |       2 00150 - INTERVAL TSO USER RESOURCE OVERLOAD                                            |WARNING     |
                |       1 00002 - INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                              |WARNING     |
-------------------------------------------------------------------------------------------------------------------------------*
```

Figure 2-4. Management Area Exception Summary Report Sample

2.2.4 Full Exception Detail

This report provides a detailed list of the exceptions that have been detected. The report is produced as an output of the CA MICS Information Center Facility described in the MICF Reference Guide and the MICF User Guide.

The purpose of the report is to provide the detail data pertaining to the identification and time of occurrence of the exceptions. The report may be selectively produced using any of the following selection criteria through online inquiry:

- Exception Number
- Severity Level
- Management Area
- Computing System Identification
- Standard Date, Time, Day, etc.

Figure 2-5 illustrates the format of this report. The heading shows the report title, system and unit database being reported on, date the report was run, and the time period being reported (Report Date) as well as the name of your company and product identification.

The body of the report consists of two lines for each exception which identifies the date and time of exception occurrence, the severity level and management area applicable to this exception, the user ID when applicable, the SAS Timespan, File Name, and record observation number identifying the source database record from which the exception was derived, the program and command name when applicable, and the exception level number and descriptive message text identifying the exception. The second line displays statistics pertinent to analyzing the exception reported.

A unique feature of this report is the provision of the Time-Period, File Name, and record observation number. With these three items it is possible for the analyst to directly examine the data record from which the exception was detected. In other words, the source record may be retrieved with no file processing! With these items the record may be directly retrieved and its contents analyzed in-depth online through SAS enabling the analyst to perform the most detailed of examinations.

This report is not a standard report and is processed as-required to provide the necessary background detail for effective analysis of the reported exceptions.

```
*-------------------------------------------------------------------------------------------------------------------*
|  CA MICS                                  Y O U R   C O M P A N Y   N A M E                          PAGE 00001 |
|                                                FULL EXCEPTION DETAIL                                              |
| DATABASE: PRIMARY                                                          RUN DATE: WEDNESDAY, MARCH 1, 2000     |
|   SYSTEM: SYSP - PRODUCTION-TSO MACHINE                                 REPORT DATE: TUESDAY, FEBRUARY 29, 2000   |
|-------------------------------------------------------------------------------------------------------------------|
| DATE/TIME SEVERITY    ID       TIMESPAN  PROGRAM  E X C E P T I O N                                               |
| INFO-AREA MGMT-AREA      OBS-NO FILE     COMMAND       NUMBER DESCRIPTION                                         |
|-------------------------------------------------------------------------------------------------------------------|
|  29FEB00                                                                                                          |
|                                                                                                                   |
|  9:10:09  WARNING     ZRX001    DETAIL                 00150 INTERVAL TSO USER RESOURCE OVERLOAD                  |
|  TSO       WORKLOAD       2674  TSOUSR01                     CPU TIME(HH:MM:SS)=00:14:11, EXCPS=008645, SU=0231012  |
|                                                                                                                   |
|  9:19:11  WARNING     ODM322    DETAIL                 00150 INTERVAL TSO USER RESOURCE OVERLOAD                  |
|  TSO       WORKLOAD       2925  TSOUSR01                     CPU TIME(HH:MM:SS)=00:05:39, EXCPS=004903, SU=0078448  |
|                                                                                                                   |
|  9:20:36  IMPACTING   POS001    DETAIL   TSOTIX        00001 INTERACTIVE TSO RUN EXCEEDED ELAPSED TIME STANDARD   |
|  TSO       STANDARDS       115  TSOINT01 CALL               ELAPSED TIME(HH:MM:SS)=01:17:23                    |
|                                                                                                                   |
|  9:22:12  WARNING     ODM322    DETAIL                 00150 INTERVAL TSO USER RESOURCE OVERLOAD                  |
|  TSO       WORKLOAD       3010  TSOUSR01                     CPU TIME(HH:MM:SS)=00:09:56, EXCPS=009588, SU=0178904  |
|                                                                                                                   |
|  9:22:12  IMPACTING   QRS001    DETAIL   READY         00001 INTERACTIVE TSO RUN EXCEEDED ELAPSED TIME STANDARD   |
|  TSO       STANDARDS       117  TSOINT01 CALL               ELAPSED TIME(HH:MM:SS)=01:43:04                    |
|                                                                                                                   |
+-------------------------------------------------------------------------------------------------------------------*
```

Figure 2-5. Full Exception Detail Report Sample

2.2.5 Short Exception Detail

Figure 2-6 illustrates the short version of the Exception Detail report. This report is identical to the Full Exception Detail with the exception that the descriptive text message has been eliminated to enable the report to be displayed online within a 72-character output line.

Note: For additional information on format, use, etc., reference the previous section describing the Full Exception Detail.

```
+--------------------------------------------------------------------+
|            Y O U R    C O M P A N Y    N A M E                     |
| CA MICS                                                      1     |
| SHORT EXCEPTION DETAIL                                             |
|    DATABASE: PRIMARY                                               |
|      SYSTEM: SYSP - PRODUCTION-TSO MACHINE                         |
| REPORT DATE:    Wednesday, Mar  1, 2000                            |
|    RUN DATE:      Tuesday, Feb 29, 2000                            |
|--------------------------------------------------------------------|
| DATE/TIME SEVERITY    ID       TIMESPAN  PROGRAM  E X C E P T I O N |
| INFO-AREA MGMT-AREA     OBS-NO  FILE     COMMAND    LEVEL NUMBER   |
|--------------------------------------------------------------------|
|  29FEB00                                                           |
|                                                                    |
|  9:10:09  WARNING     ZRX001    DETAIL                   00150     |
|  TSO       WORKLOAD       2674  TSOUSR01                           |
|                                                                    |
|  9:19:11  WARNING     ODM322    DETAIL                   00150     |
|  TSO       WORKLOAD       2925  TSOUSR01                           |
|                                                                    |
|  9:20:36  IMPACTING   POS001    DETAIL   TSOTIQ          00001     |
|  TSO       STANDARDS       115  TSOINT01 CALL                      |
|                                                                    |
|  9:22:12  WARNING     ODM322    DETAIL                   00150     |
|  TSO       WORKLOAD       3010  TSOUSR01                           |
|                                                                    |
|  9:22:12  IMPACTING   QRS001    DETAIL   READY           00001     |
|  TSO       STANDARDS       117  TSOINT01 CALL                      |
|                                                                    |
+--------------------------------------------------------------------+
```

Figure 2-6. Short Exception Detail Report Sample

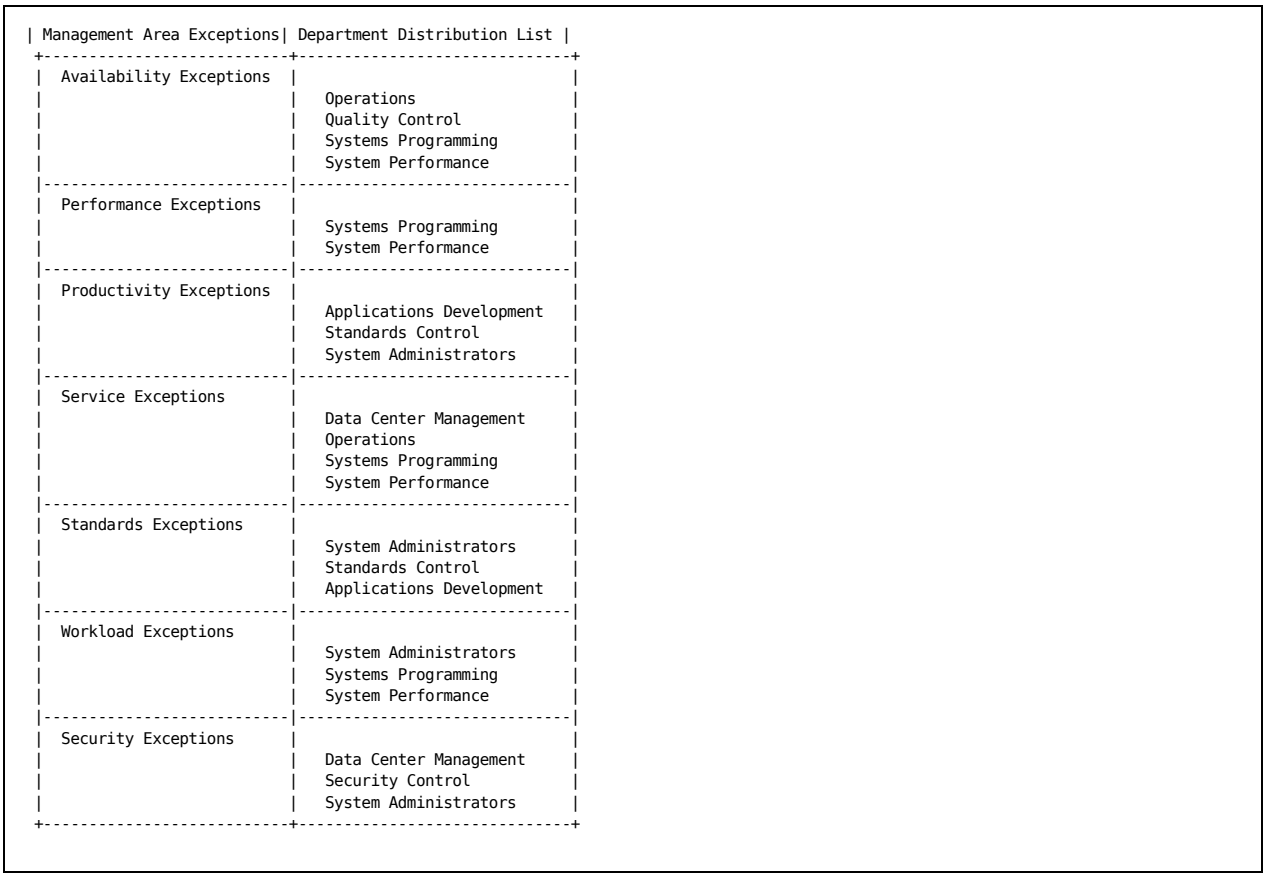
2.3 Using Exception Reports

The five standard and inquiry exception reports have been identified and described in previous sections in this chapter. This section suggests a plan for the distribution and use of the exception reports. This is intended only to aid you in developing the plan most consistent with your individual environment.

The Exception Management Overview should be made available to the data center managers having responsibility for system availability, operation, or performance.

The Severity Level Exception Summary should be generated specifically for use by the System Performance Department. The report should contain a prioritized list of all critical, impacting, and warning exceptions. A copy of the critical exceptions report should be distributed to the same managers receiving the Exception Management Overview.

The Management Area Exception Summary should be separated by area reported (e.g., availability) and distributed as illustrated in Figure 2-7.



Management Area Exceptions	Department Distribution List
Availability Exceptions	Operations
	Quality Control
	Systems Programming
	System Performance
Performance Exceptions	Systems Programming
	System Performance
Productivity Exceptions	Applications Development
	Standards Control
	System Administrators
Service Exceptions	Data Center Management
	Operations
	Systems Programming
	System Performance
Standards Exceptions	System Administrators
	Standards Control
	Applications Development
Workload Exceptions	System Administrators
	Systems Programming
	System Performance
Security Exceptions	Data Center Management
	Security Control
	System Administrators

Figure 2-7. Management Area Exception Report Distribution

The Full and Short Exception Detail reports are produced on an as-required basis using Online Inquiry. These reports are selectively generated to provide the required detail to support the findings in the summary reports.

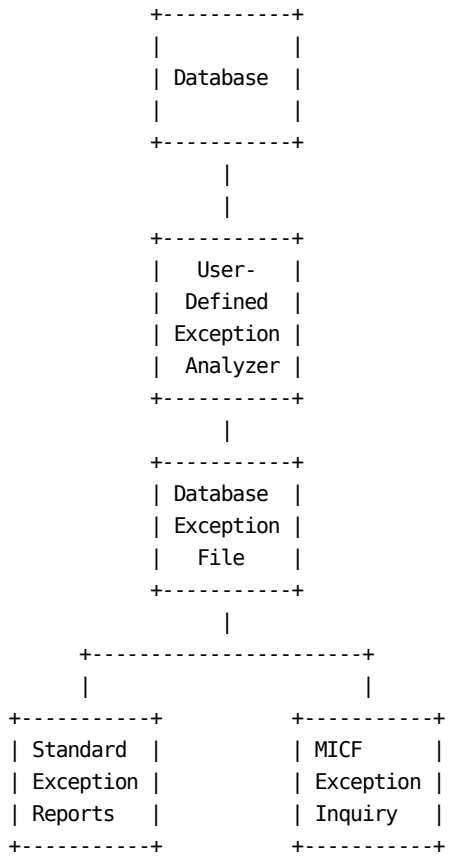
The following represents a sample of the types of online inquiry selection that may prove useful:

- Selection of a specific exception or set of exceptions
- Selection of a user or user group
- Selection by severity level
- Selection by information area
- Selection by date and/or time of occurrence

These selection facilities are useful in analyzing sets of exceptions; for in-depth analysis of certain exception types; selective reporting to analyze a particular user, user department, or group; and for tailoring exception reports for internal reporting needs.

2.4 Exception Values

Figure 2-8 illustrates the operation of the Exception Reports process. The Database, Database Exception File, Standard Exception Reports, and MICF Exception Inquiry are standard parts of this process. The User-Defined Exception Analyzer comprises the part of this system which tailors and modifies the exceptions to uniquely address an installation's requirements.



The exceptions are defined with each product and a starter set of default values is provided. It is the responsibility of each installation to review this starter set and modify the values used for exception identification to adjust them for applicability to your environment and requirements.

The exception values are defined in a single source member for each CA MICS product (e.g., TSO, RMF, SMF) in the CA MICS source library (e.g., prefix.MICS.USER.SOURCE). An exception group exists for each unique file that is to be processed by the Exception Analyzer and consists of the exceptions which are to be processed using a specific file.

ABOUT EXCEPTION TESTS

An exception test defines the tests performed to determine whether or not an exception condition exists and needs to be reported. The test also states the exception's identifying number and its severity and management levels. You can modify, and in some cases add, values to adjust the exception test to meet your installation's requirements.

Exception tests reside in sharedprefix.MICS.SOURCE, in modules named DYcccEXC, where ccc is the three-character product identifier.

The exception code is organized sequentially by exception number within the member. Each exception condition consists of the standard identification definition (e.g., severity level), exception-dependent criteria (e.g., amount of CPU time used), and standard selection facilities (e.g., selection of prime-time hours only). To modify an exception, locate it by name or number, then change the value directly in the code.

Refer to the Exceptions chapter of the individual product guides for detailed exception information for the products licensed by your site.

EXCEPTION VALUE ANALYSIS

The Exception Value Analysis Process is a procedure by which the CA MICS Database is used to determine the values to be used for exceptions. Figure 2-9 illustrates the operation of the Exception Value Analysis Process. The Exception Value Analyzer extracts values from the database for those exception values which are to be analyzed. Descriptive statistics for the selected variables are printed in the Exception Value Analysis Report.

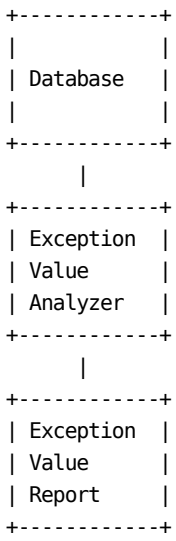


Figure 2-9. Exception Value Analysis Operational Flow

EXCEPTION VALUE ANALYSIS REPORTS

Exception Value Analysis Reports help you determine the values to use in the exception tests coded in DYcccEXC. There is one report available for each CA MICS product. The code to produce the report is located in sharedprefix.MICS.SOURCE(cccEVA), where ccc is the three-character product identifier.

For each data element used in an exception test, this report shows twelve statistical measures, described below. It also shows a recommended value.

Figure 2-10 illustrates the format of this report. The heading shows the report title, system being reported on, the date on which the report was run, and company and product identification.

The body of the report is grouped by exception number. After the exception number and name, the report shows the data elements used in the exception test. For each element, the report gives its name and descriptive title. Some exception data elements are repeated for sub-groups of exception tests. (e.g., disk or tape). For these exceptions a qualifier is shown. The number of observations used to calculate the measures are printed.

The statistical measures are divided into three types: basic, standard deviations, and percentiles. Basic statistical values are the minimum, mean, median, and maximum values. Standard deviation values are the mean plus and minus one and two standard deviations. Percentile values include the 1st, 5th, 95th, and 99th percentile values.

The CA MICS SUGGESTED VALUE is the system's choice of the statistical function (e.g., 99th percentile) that most closely meets the requirement. This value provides you with a representative initial exception value.

The INDUSTRY RECOMMENDED VALUE is not supported at this time.

```
CA MICS                                   Y O U R   C O M P A N Y   N A M E                                  PAGE     1
                                                EXCEPTION VALUE ANALYSIS
 SYSTEM: SYSP - PRODUCTION TSO                                                          RUN DATE:     WEDNESDAY, OCT 4, 2000
 INFORMATION AREA: TSO
-----------------------------------------------------------------------------------------------------------------------------|
 EXCEPTION   | QUALIFIER /   | EXCEPTION DESCRIPTION /                                                                       |
 NUMBER      | DATA ELEMENT  |      DATA ELEMENT DESCRIPTION AND STATISTICAL VALUES                                          |
-----------------------------+-----------------------------------------------------------------------------------------------|
 00001                       | INTERACTIVE TSO RUN EXCEEDED ELAPSED TIME STANDARD                                            |
              TSIELPTM       |        EXECUTION ELAPSED TIME                                          OBSERVATIONS:      632 |
                             |-----------------------------------------------------------------------------------------------|
 BASIC STATISTICAL VALUES:   |   MIN:          0.020   |   MEAN:       690.425  |   MEDIAN:     110.660  |   MAX:       5079.387  |
 STANDARD DEVIATION VALUES:  |    -2:           .      |    -1:           .     |    +1:       1862.770  |    +2:       3035.115  |
 PERCENTILE VALUES:          |   1ST:          0.289   |   5TH:          1.180  |   95TH:      3650.541  | > 99TH:      4448.140< |
                            *-----------------------------------------------------------------------------------------------|
 INDUSTRY RECOMMENDED VALUE:   N/A          CA MICS SUGGESTED VALUE:            1:14:08  HH:MM:SS (              4448 SECONDS)   |
-----------------------------------------------------------------------------------------------------------------------------|
 00002                       | INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                                             |
              TSICPUTM       |        CPU TIME CONSUMED                                               OBSERVATIONS:      632 |
                             |-----------------------------------------------------------------------------------------------|
 BASIC STATISTICAL VALUES:   |   MIN:          0.010   |   MEAN:         1.752  |   MEDIAN:       0.300  |   MAX:         87.789  |
 STANDARD DEVIATION VALUES:  |    -2:           .      |    -1:           .     |    +1:         8.189  |    +2:         14.626  |
 PERCENTILE VALUES:          |   1ST:          0.020   |   5TH:          0.060  |   95TH:        5.162  | > 99TH:        30.047< |
                            *-----------------------------------------------------------------------------------------------|
 INDUSTRY RECOMMENDED VALUE:   N/A          CA MICS SUGGESTED VALUE:            0:00:30  HH:MM:SS (                30 SECONDS)   |
-----------------------------------------------------------------------------------------------------------------------------|
 00002                       | INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                                             |
              TSIEXCPS       |        I/O (EXCP S) GENERATED                                          OBSERVATIONS:      632 |
                             |-----------------------------------------------------------------------------------------------|
 BASIC STATISTICAL VALUES:   |   MIN:          0.000   |   MEAN:       293.239  |   MEDIAN:      12.000  |   MAX:      38261.000  |
 STANDARD DEVIATION VALUES:  |    -2:           .      |    -1:           .     |    +1:       2028.385  |    +2:       3763.532  |
 PERCENTILE VALUES:          |   1ST:          0.000   |   5TH:          0.000  |   95TH:      1084.599  | > 99TH:      3662.348< |
                            *-----------------------------------------------------------------------------------------------|
 INDUSTRY RECOMMENDED VALUE:   N/A            CA MICS SUGGESTED VALUE:              3662                                   |
-----------------------------------------------------------------------------------------------------------------------------|
 00002                       | INTERACTIVE TSO RUN EXCEEDED RESOURCE USAGE LIMIT                                             |
              TSISERVU       |        SERVICE UNITS                                                   OBSERVATIONS:      632 |
                             |-----------------------------------------------------------------------------------------------|
 BASIC STATISTICAL VALUES:   |   MIN:          0.000   |   MEAN:     13749.310  |   MEDIAN:    2005.000  |   MAX:     903687.000  |
 STANDARD DEVIATION VALUES:  |    -2:           .      |    -1:           .     |    +1:      68567.899  |    +2:     123386.489  |
 PERCENTILE VALUES:          |   1ST:          0.000   |   5TH:        150.600  |   95TH:     42008.693  | > 99TH:    228175 497< |
                            *-----------------------------------------------------------------------------------------------|
 INDUSTRY RECOMMENDED VALUE:   N/A            CA MICS SUGGESTED VALUE:            228175                                 |
-----------------------------------------------------------------------------------------------------------------------------|
 00103                       | INTERVAL TSO SYSTEM RESOURCE OVERLOAD                                                         |
              TSOEXCPS       |        I/O (EXCP S) GENERATED                                          OBSERVATIONS:      197 |
                             |-----------------------------------------------------------------------------------------------|
 BASIC STATISTICAL VALUES:   |   MIN:        884.000   |   MEAN:      4808.061  |   MEDIAN:    3985.000  |   MAX:      23258.000  |
 STANDARD DEVIATION VALUES:  |    -2:           .      |    -1:       1490.541  |    +1:       8125.581  |    +2:      11443.101  |
 PERCENTILE VALUES:          |   1ST:       1027.560   |   5TH:       1639.700  |   95TH:     10394.994  | > 99TH:     20619.471< |
                            *-----------------------------------------------------------------------------------------------|
 INDUSTRY RECOMMENDED VALUE:   N/A            CA MICS SUGGESTED VALUE:            20619                                  |
-----------------------------------------------------------------------------------------------------------------------------|
```

EXCEPTION VALUE ANALYSIS ROUTINES

The Exception Value Analysis routines are defined in sharedprefix.MICS.SOURCE(cccEVA) as described in the prior section. An exception group exists for each file that is to be processed by the Exception Value Analyzer.

The job control to execute the EVA process is contained in the prefix.MICS.CNTL library. Each product has a separate member in the library; member names are cccEVA, where ccc is the product's three-letter identifier.

To perform an analysis of exception values for a product, submit the applicable job from the prefix.MICS.CNTL library:

```
SUB 'prefix.MICS.CNTL(cccEVA)'
```

ASSIGNING EXCEPTION VALUES

The procedure below describes adjusting the values used by the CA MICS Exception Analyzers.

1. Identify the exceptions you want to change.

2. List the Exception Analyzer member in sharedprefix.MICS.SOURCE(DYcccEXC), where ccc is the product identifier.

3. Execute the applicable Exception Value Analysis job according to the instructions provided in the previous section.

4. Using the source listing of the Exception Analyzer and the corresponding Exception Value Analysis Report, mark up the source listing with the new exception values. The exceptions are ordered by number.

5. Copy the routine to be changed to a test library and make the changes.

6. Test the routine by executing it to ensure that there are no syntax errors.

7. Copy the modified source member back to the production user source library, prefix.MICS.USER.SOURCE, maintaining the original copy in the sharedprefix.MICS.SOURCE library.

8. Monitor the next day's production execution of the exception reports to ensure that the adjustments have been correctly implemented.