

SECTION 1

Netview ADMINISTRATION, policies, and procedures

Identify and evaluate the controls and management practices for the administration of NetView monitoring tool.

Consider and Document:

Organization Structure

- 1.1 *Obtain the organization chart for the Telecommunications Services Division (TSD) is responsible for NetView, such as changing installation parameters to achieve effective response times and implementing software exists, etc. Determine whether a proper segregation of duties exists.*

Standards and Procedures

- 1.2 *Obtain a copy of the daily operational standards and procedures and evaluate for adequacy. Procedures should include :*
- *NetView management operating procedures, including remote access procedures.*
 - *NetView status alerts.*
 - *Problem monitoring and resolution management.*
- 1.3 *Evaluate the process for security administration (e.g., adding/deleting users, distribution of NetView security violation reporting, and access to critical system and production Network objects.).*

SECTION 2

NetView Components

NetView is a IBM tool used by TSD in operation and monitoring of the telecommunication network.

Consider and document:

2.1 Identify and evaluate the NetView components for appropriate integrity controls.

The Command Facility

- *Message routing*
- *Access to disruption Network commands*

The Session Monitor error conditions

- *Session termination, activation and recycling*
- *Lost messages*
- *Destination problems*

The Hardware Monitor

- *Statistics*
- *Events*
- *Alerts*

The Status Monitor

- *Allows domain viewing by the Network Operator*
- *Determine which alerts have been given the highest priority*

SECTION 3

NetView Facilities

NetView provides the operator with the facilities and capability for managing and controlling all of the resources in the network from a central point of control.

Consider and document

- 3.1 *How is the hardware status monitor Network Problem Determination Application (NPDA) utilized within NetView.*
- 3.2 *Describe the use of **Static** and Dynamic Alerts.*
- 3.3 *Determine if session data Network Logical Data Monitor (NLDM) is being utilized within the Network Communication Control Facility (NCCF). Which sub-functions are used in problem determination for LUs PUs and SSCPs configs.*
- 3.4 *Determine how Network Control Center (NCC) uses Netview NCCF facilities in VTAM. Activating LU/PU/LINKS/LINES/MAJNODES. Have clist been developed for activation automation?*
- 3.5 *Review the use of the Status Monitor Function STATMON in Netview. Are NCPs coded to support STATMON.*
- 3.6 *Is the Help desk Function being utilized in Netview or similar software solution in place for inquiries into a user problem.*
- 3.7 *Obtain and review NETVIEW initialization parameters, operator profiles, and system command files.*

Operator profiles are coded on 'DSIOPF' by TSD.

 - a) *Determine that access is appropriate within the given CLASSES within commands to RACF.*
 - b) *Determine that external software is linked for password clearance.*
 - c) *Evaluate privileged IDs within NETVIEW.*

- d) *Determine that operations, tech support, and help desk personnel are granted only those commands necessary to perform their function.*
- e) *Determine if monitoring and reporting are utilized.*

SECTION 4 EXTERNAL SECURITY LINKS(RACF, EXITS,USER PRIVELEGES)

Evaluate Logical Security Controls used to protect the NetView Environment.

Consider and document:

- 4.1 *Obtain a copy of the 'DSIOPF' member that contains operator profiles which restricts the Netview operator functions. Also obtain 'DSICMD' that defines the commands an operator can issue. Evaluate operator capabilities.*
 - Operator span of control.*
 - Scope of NetView commands.*
 - NetView parameters.*
 - Restriction of the NetView operator.*
- 4.2 *Using the RACF list dataset, obtain RACF profiles for the above data sets and evaluate for appropriateness.*
- 4.3 *Obtain the JCL used to start NetView. Review the list with the appropriate manager and determine that NetView start-up routines are include in the JCL.*
- 4.4 *Determine who has 'update' or 'alter' access to data sets specified in the start jobs in 4.3.*

SECTION 5 SYSTEM INITIALIZATION, DEFINITIONS, AND UTILITIES

The purpose of this test is to evaluate the RACF interface controls. All steps should be executed against MVS production image at Barclay and at Teaneck.

Evaluate Logical Security Controls used to protect the NetView Environment.

Consider and document:

- 5.1 Review the NetView system interface parameters and determine if the installation-elected options are appropriate and provide adequate controls.*

- 5.2 Determine if RACF is protecting all control regions, production libraries and data sets, and classes for NetView. Using RACF Command or Panels, determine the authority granted and note any high level authorities which exist as attributes or established by connected groups.*

- 5.3 Review the procedures and forms, and approval requirements for adding, deleting, or modifying NetView interface system options.*

- 5.4 Are dial-up lines controlled by either an automatic callback procedure or TelNet/Sprint (manual intercept) by operations personnel at the data center*

- 5.5 Is access to system terminals controlled by a front-end tool such as Netview Access Services Facility (NAS).*

SECTION 1

SDSF - ADMINISTRATION, POLICIES AND PROCEDURES

SDSF is an IBM program product that allows authorized users to monitor and control the operation of MVS/JES2 system. SDSF consists of panels that provide immediate information about jobs, printers, queues, and resources in an MVS/JES2 system. From these panels, authorized users can enter SDSF commands to control the processing of jobs and the operation of systems resources. Authorized users can issue MVS and JES2 system commands from the SDSF panels.

Objective: To ensure that SDSF functions are adequately restricted.

Consider and Document:

Organization Structure

- 1.1 *Obtain the organization chart for the MVS System Software department responsible for SDSF customization. Determine whether a proper segregation of duties exists.*

Standards and Procedures

- 1.2 *Obtain a copy of the SDSF operational standards and procedures and evaluate for adequacy. Procedures should include :*
 - *Policy governing the assignment of SDSF authorities ;*
 - *SDSF authorities controlled via external security package ;*
 - *Bank policy on the confidentiality of reports ; and*
 - *Problem monitoring and resolution management.*
- 1.3 *Evaluate the process for security administration (e.g., adding/deleting users, distribution of SDSF security violation reporting, and access to critical system and production SDSF objects,).*

SECTION 2

PROTECTED SDSF RESOURCES

Objective:

To ensure that adequate security procedures have been established to prevent unauthorized SDSF execution.

Consider and document

- 2.1 *Is SDSF linked to a external security package such as RACF to control access to the following resources:*
 - SDSF panels.*
 - SDSF authorized commands.*
 - Use of the /command to issue MVS and JES2 commands.*
 - Overtimeable fields.*
 - Destination names.*
 - Operator authority by destination.*
 - Initiators.*
 - Printers.*
 - Jobs affected by action characters and overtimeable fields.*
 - Output groups affected by action characters and overtimeable fields.*
 - SYSIN/SYSOUT data sets for browsing and viewing.*
 - MVS and JES2 commands that are generated by action characters and overtimeable fields.*

SECTION 3 REQUIRED PARAMETERS AND DEFINITIONS

Evaluate Logical Security Controls used to protect resources under the SDSF environment

Consider and document:

3.1 *Obtain the most recent ISFPARMS assembly and link edit listing and check to see if following parameters are appropriately set:*

- ISFPMAC (see 3.3)
- ISFGRP (see 3.2)
- CMDLEV (see 3.3)
- CMDAUTH (see 3.3)
- ISFNTBL
- ISFFLD

3.2 *Identify all the users and groups defined in the SDSF environment. Users are defined via the ISEGRP macros.*

Identify users characteristics assigned:

3.3 *If RACF security is used, the following ISFPARMS macros are required ensure that they are appropriately set:*

ISFPMAC, for initialization.

ISFPMAC defines all global initialization parameters and includes limits for various SDSF commands that users issue, the prefix of the JES2 spool dataset, the name of the SDSF panel dataset, the number of buffers for each user, and the largest screen size that will be used.

ISFGRP, for group membership and authorization parameters, sub-parameters (AUTH, CMDAUTH, and CMDLEV) determine their respective SDSF authorities. CMDLEV, indicates the MVS and JES2 commands that a member of the group may issue from the SDSF command. Ordinary TSO users should have CMDAUTH =(NOTIFY,USERID) CMDLEV =(2).

3.4 *Identify the commands that a user can initiate from the command line.*

SECTION 4 SYSTEM INITIALIZATION, DEFINITIONS, AND SECURITY INTERFACE

The purpose of this test is to evaluate the RACF interface controls. The following steps should be done on the production environment for both Barclay and Teaneck.

Evaluate Logical Security Controls used to protect the SDSF Environment.

Consider and document:

4.1 *Describe the process that used by RACF to authenticate SDSF users, such as:*

- *User attempts to access an SDSF resource.*
- *RACF gives an indeterminate response because the resource class is not active.*
- *RACF gives an indeterminate response because there are no profiles that match the authorization request.*

4.2 *Obtain and identify SDSF resource class for 101B and Teaneck. Using TSO (RL - Resource List) class for each entity evaluate access privileges. (e.g. Log access, MVS console, command authority, etc.).*

4.3 *Determine if RACF access logs are kept to protect SDSF resources based on auditing setting in the RACF profile for the resource.*

Identify System Management Facility (SMF) records that are kept and analyzed each event:

- Accounting*
- Datasets*
- Volume*
- System*
- Subsystem*

SECTION 1 OMEGAMON ADMINISTRATION, POLICIES AND PROCEDURES

OMEGAMON for MVS is a System Management tool used by the Bank at 101B and Teaneck for performance evaluation and problem resolution. OMEGAMON is supported by the Systems Software Department, Systems Optimization Section.

OMEGAMON provides a consolidated view of the MVS system and allows users to analyze, control, and dynamically modify the MVS/JES system. OMEGAMON displays how efficiently the operating system is working and points the user to the areas where changes could improve system performance. OMEGAMON is also a performance tool that provides comprehensive real-time problem isolation and analysis, and then provides recommendations to safeguard availability and response time.

Objective:

Identify and evaluate the controls and management practices for the administration of OMEGAMON.

Consider and Document:

Organization Structure

- 1.1 *Obtain the organization chart for the System Optimization department responsible for OMEGAMON. Determine whether a proper segregation of duties exists.*

Standards and Procedures

- 1.2 *Obtain a copy of the daily operational standards and procedures and evaluate for adequacy. Procedures should include :*
 - *OMEGAMON management operating procedures.*
 - *OMEGAMON Installation and Customization.*
 - *Problem monitoring and resolution management.*
- 1.3 *Evaluate the process for security administration (e.g., adding/deleting users, distribution of OMEGAMON security violation reporting, and access to critical system and production OMEGAMON objects).*

SECTION 2 OMEGAMON ENVIRONMENT AND SECURITY CONTROLS

Ensure that adequate security procedures have been established over OMEGAMON.

Consider and document:

1. *Identify the OMEGAMON environment and controls regarding the availability and access to OMEGAMON commands.*
 - a. *Determine whether powerful OMEGAMON commands can be used at this site. These commands are provided only when OMEGAMON product has been installed as APF authorized.*
 - b. *Obtain the listing for the OMEGAMON security update program - 'OMSECUP', using the control statements of 'LIST=YES', 'UPDATE=NO'.*
 - c. *To determine the type of security used, note the setting for the 'MODULE = ' control statement.*
 - d. *Obtain and review the source code for the exit routine defined in the 'MODULE = ' control statement. Ascertain what impact the active exit routine has on security for OMEGAMON environment at BNY.*
2. *Determine whether access to the OMEGAMON commands are adequately controlled and are they provided only on an as needed basis.*
 - a. *Using the listing for the OMEGAMON security update program - 'OMSECUP' obtained in the previous step, review the command control statement specifications set for sensitive OMEGAMON Commands. These commands include:*
 - DSA - sets and displays authorization to list or zap non-sharable data-only spaces;
 - APFU - updates the APF library list;
 - CONS - displays the MVS operator console;
 - KILL - terminates an address space;
 - LPAM - adds, deletes or lists LPA members;
 - MCHN - scans common area tables;
 - MLIST - displays storage;
 - MSCN - scans storage;
 - MZAP - modifies storage;
 - OCMD - executes MVS or JES2 primary console commands;

- PEEK - collects information about a single address space;
- SCHN - scans data-only spaces;
- SSCN - scans data-only space storage;
- SZAP - modifies the content of data-only space storage;
- XMLS - displays MVS storage;
- XMSC - scans internal table;
- XMZP - modifies storage;
- ALIB - (minor command of the SYS command) - displays the defined APF library names.
- MNSW (minor command) - marks job as non-swappable;

b. For the sensitive OMEGAMON command authorities (identified in the above procedure), evaluate whether access has been provided only to those individuals that require it in performing their daily job functions.

c. Review the OMEGAMON resource class rules (type OMS) that control these commands for which external security is being activated.

3. Verify that the OMEGAMON product library has adequate data set protection.

a. Obtain the name of the OMEGAMON executable libraries. Also, using the listing for the OMEGAMON security update program - 'OMSECUP', obtained in the first audit step, obtain the name of the data set specified on the 'AUTHLIB=' control statement

b. Determine the individuals that are directly responsible for maintaining the product (i.e. system programmers).

c. Examine the data set access rules/profiles to ensure that update access to the OMEGAMON executable library and the AUTHLIB data set are restricted only to those individuals directly responsible for maintaining the product.

SECTION 3 SYSTEM EVENT TRAILS

System Management Facility (SMF) is a component of the MVS system that journals information about specific events. Events that may be recorded are beginning and ending jobs, job steps, and opening and closing of data sets. Data from SMF can be used for adjusting hardware and system software configuration.

1. *Describe the system configuration and SMF options in effect, that provide system statistics, and record the occurrence of specific events.*
2. *Obtain a list of the SMF options specified in the SMFPRMxx member of SYS1.PARMLIB.*

Identify System Management Facility records that are kept and analyzed for each event recorded:

- *Accounting*
- *Dataset*
- *Volume*
- *System*
- *Subsystem*

3. *Determine those subsystem activities and events are recorded and any questionable entry is researched, corrected, and management reviewed, e.g., TSO, JES, and Security software.*

Step Performed by _____

Date _____

I:\SYSAUD\7G890\NETV_PGM.DOC