Auditing z/OS

to

Generally Accepted
Security Practices (GASP)

VERSION 1

by Julie Bergh

7/29/22

Foreword

There are many z/OS Security practices. Quite often which one or which set of them is needed to establish a control or mitigate a discovered vulnerability will depend on the opinion of those that offer advice on such matters. There are, in fact, so many solutions to any given security concern that Auditors and those new to z/OS security are often frustrated and confused over which is best, which is most appropriate, best fitting to the situation at hand.

Unlike professional accountants who can rely on the long standing rubric of Generally Accepted Accounting Practices (GAAP) as a basis to measure their actions and client processes, there is no such a standard for z/OS Security professionals to follow. The z Exchange seeks to resolve this void and address the z/OS skills challenge head on by opening up to our community a conversation that we hope will culminate in a first ever statement of Generally Accepted Security Practices (GASP) for z/OS.

To begin the process, we will rely on the experience and insights of Julie Bergh. Well known within z/OS security circles, with well over 20 years of hands-on experience in applying z/OS security solutions, she has graciously stepped up to share her knowledge and take the first shot in this Version 1 of Generally Accepted Security Practices. This is her work and is presented to encourage your contribution to what we hope will be an ongoing professional and productive conversation.

Jerry Seefeldt
Director of Strategic Partnerships
NewEra Software, Inc.
Moderator and Custodian of The z Exchange Resources

RACF System Options

During the years I have met with many clients to discuss mainframe security. During this time a frequent topic is what the Auditors commented on during a recent audit. When Auditors are looking at RACF z/OS environments, they usually ask for the data security monitor (DSMON) report and a listing of the RACF system options (SETROPTS). SETROPTS stands for SET RACF OPTIONS. This document will focus on the RACF system options.

The client provides the Auditors with a listing (e.g., maybe a text file) for them to review. To obtain the complete listing of SETOPTS the person needs to have the RACF SYSTEM SPECIAL or RACF ROAUDIT attribute on their userid.

These are what I call Generally Accepted Security Practices (GASP). Many times client will ask for 'best practices' Many will use the Security Technical Implementation Guide (STIG). Many of the generally accepted security practices are very close to what is recommended with the STIG controls.

Below is an abbreviated list of what a SETROPTS report looks like. As one will notice it is just a listing of the options. There are specific areas that Auditors will check, and I usually describe them with the following:

- Attributes
- Audit / Log Options / Statistics
- Classes – Active, Generic Commands, Generic Profiles, RACLIST, GENLIST, Global Checking
- Data Protection
- Password
- User Activity
- JES
- Mandatory / Discretionary Controls
- General

In addition, Auditors will also ask for what is called the 'DSMON' report. This is described below.

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
1	**ATTRIBUTES = INITSTATS**	
	• Specifies that statistics available during RACF user verification are to be recorded. • Includes statistics like the date and time the user was verified by RACF. • If you specify INACTIVE, REVOKE, HISTORY, or WARNING, INITSTATS must be in effect. • INITSTATS is in effect when RACF is using a newly-initialized database..	• INITSTATS **Auditors will check to ensure this is turned on.**
2	**ATTRIBUTES = WHEN(PROGRAM – BASIC)**	
	• WHEN (PROGRAM) Says to allow program-pathing (for example, "permit this user to update this dataset when going through the specified program"). Used also to activate the program resource class. RACF can operate in: • BASIC program security mode (default) • ENHANCED program security mode • ENHANCED-WARNING program security mode	• WHEN(PROGRAM – BASIC) at a minimum **Auditors will check to ensure this is turned on.**
3	**ATTRIBUTES = SAUDIT**	
	• RACF logs the command and request activity (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH, which are never logged) of users with the SPECIAL or group-SPECIAL attribute. • SAUDIT is in effect at RACF initialization. •	• SAUDIT • **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Auditors will check to ensure this is turned on.**
4	**ATTRIBUTES = CMDVIOL - -**	
	• RACF to logs all command violations (except for LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH, which are never logged). • CMDVIOL is in effect at RACF initialization. •	• CMDVIOL • **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Auditors will check to ensure this is turned on.**
5	**ATTRIBUTES = OPERAUDIT**	
	• OPERAUDIT, logs all accesses to RACF-protected resources granted because the user has the OPERATIONS or group-OPERATIONS attribute, and all uses of the ADDSD, and RDEFINE commands allowed because a user has the OPERATIONS or group-OPERATIONS attribute. • NOOPERAUDIT is in effect is initialized RACF database •	• OPERAUDIT • **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Auditors will check to ensure this is turned on.**
6	**ATTRIBUTES = TERMINAL(READ)**	
	• TERMINAL(READ or NONE) - is used to set the UACC associated with undefined terminals. • Only appears if the TERMINAL class is active • If you specify TERMINAL but do not specify READ or NONE, the system prompts you for a value. •	• Leave TERMINAL set at READ (IF NEEDED) **This is being checked more from an Auditors viewpoint.**
7	**STATISTICS =**	
	Using the SETROPTS STATISTICS option does the following: • Specifies which RACF classes are to keep record counts. This is only for discrete profiles and does not keep counts for RACLISTed classes. •	• Since statistics applies only to discrete profiles, don't worry about it. **Some Auditors will check this and as is described above, this is not an audit finding.**
8	**AUDIT CLASSESS = ??**	
	• Specifies the names of the classes for which you want RACF to perform auditing. •	• Turn on audit for every resource class since you need to know who made each and every change to a rules • NOTE: This switch does not cause logging for resource checks, only for changes to rules • **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Auditors will check to ensure this is turned on.**

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
9	**ACTIVE CLASSESS = ?? -**	
	• Specifies classes for which RACF checking is to be in effect. • If you activate a class using SETROPTS CLASSACT, RACF activates all classes in the class descriptor table that have the same POSIT value as the class you specify. •	• Make active only those classes you are ready to administer. **Auditors will check various classes.**
10	**GENERIC PROFILE CLASSES = ??**	
	• GENERIC PROFILE--- Specifies classes for % and * are to be treated as wildcard characters. •	• Turn on generic profile for every class possible (not possible for group classes). **Auditors will check to ensure this is turned on.**
11	**GENERIC COMMAND CLASSESS = ?? -**	
	• Activates generic profile command processing for the specified classes. •	• Turn on generic command for those classes you want to allow generics **Auditors will check to ensure this is turned on.**
12	**GENLIST CLASSESS = ??**	
	• Specifies classes for which RACF is to keep all the generic profiles locked into common storage instead of private storage. Check with systems programmer before activating this over RACLIST. • NOTE: cannot specify GENLIST and RACLIST for the same class. •	• Use GENLIST where possibly needed for performance. • Mainly used for VM classes • Otherwise this is usually ignored and RACLIST is used in place. **Not usually checked by Auditors**
13	**GLOBAL CHECKING CLASSESS = ??**	
	• Specifies classes for which RACF is to use global checking • Global checking for classes is checked before other access checks. • Global class does not deny access.	• Use global for datasets, selecting the dataset rules carefully based upon analysis of frequency of use and sensitivity. • An entry to permit any access to a dataset whose high level qualifier is your USERID would make sense. • Use global for other classes only if the frequency justifies. **Auditors will check to see which classes are in this. They will also look at this in the DSMON report described below.**
14	**RACLIST CLASSESS = ??**	
	• Specifies classes for which RACF are loaded into memory for fast reference during authorization processing. • . Class profiles are loaded into the application address space. •	• Use RACLIST for resource classes with few rules and frequent access, plus for classes which require it. **Auditors will check to ensure this is turned on for appropriate classes.**
15	**GLOBAL = YES RACLIST ONLY = ??**	
	• Specifies classes for which RACF are loaded into memory where multiple applications can share •	• Discuss with systems programmer • Some classes like CICS automatically RACLIST profiles **Auditors will check to ensure this is based on what classes are turned on.**

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
16	**LOGOPTIONS "ALWAYS" CLASSES = NONE** **LOGOPTIONS "NEVER" CLASSES = NONE** **LOGOPTIONS "SUCCESSES" CLASSES = NONE** **LOGOPTIONS "FAILURES" CLASSES = NONE** **LOGOPTIONS "DEFAULT" CLASSES = ??**	• Set logoptions to default for all classes unless you have a specific reason to set it otherwise • **SYSTEM AUDITOR to change** • **ROAUDIT to view**
	• LOGOPTIONS ALWAYS--- Specifies classes for which every reference is to be logged. • The ALWAYS operand overrides any auditing specified in profiles in the class. • LOGOPTIONS NEVER--- Specifies classes for which no reference is to be logged.Suppresses everything but UAUDIT • LOGOPTIONS SUCCESSES--- Specifies classes for which every successful reference is to be logged. • LOGOPTIONS FAILURES--- Specifies classes for which every failed reference is to be logged • LOGOPTIONS DEFAULT--- Specifies classes for which logging is based on the options in the RACF rule (GLOBALAUDIT or AUDIT).	• **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Some Auditors will check to ensure this is turned on.**
17	**AUTOMATIC DATASET PROTECTION ?????**	
	• AUTOMATIC DATASET PROTECTION--- Used to be used to specify that for certain users, every disk dataset which they create gets a RACF discrete profile with the RACF bit turned on. •	• Leave automatic dataset protection inactive **Auditors will check to ensure this is turned off.**
18	**ENHANCED GENERIC NAMING IS IN EFFECT**	
	• ENHANCED GENERIC NAMING--- Allows you to specify the '**' characters when you define dataset profile names	• Set enhanced generic naming on or off for all of your installations • Either way is fine, most clients have EGN turned on. **Most customers have this turned on. Auditors may question if this is not on.**
19	**REAL DATA SET NAMES OPTION IS INACTIVE**	
	• REAL DATASET NAMES--- Used with dataset naming conventions table to specify that un-modified versions of dataset names are to be logged. •	• Only needed if you are using the dataset naming convention exit. **Auditors will question this if something is there.**
20	**JES-BATCHALLRACF OPTION IS ??????** **JES-XBMALLRACF OPTION IS ??????** **JES-EARLYVERIFY OPTION IS ?????**	
	• **BATCHALLRACF** Specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch jobs • **XBMALLRACF** Specifies that JES is to test for the presence of either a user ID and password on the JOB statement, or JES-propagated RACF identification information for all jobs to be run with an execution batch monitor. • JES-EARLYVERIFY--- OBSOLETE, JES now always assumes that this switch is on.	• Activate BATCHALLRACF and XBMALLRACF together • Activate BATCHALLRACF and XBMALLRACF together • OBSOLETE - Don't worry about EARLYVERIFY **Auditors will review these settings. The JES-EARLYVERIFY they may want on and will need to describe why it is not needed.**
21	**PROTECT-ALL-OPTION IS ???????**	
	• PROTECT-ALL--- Requires every dataset to have a RACF rule covering it. If TAPEDSN is set, applies to tape datasets, as well. • Turn on PROTECTALL in FAIL mode •	• Turn on PROTECTALL in FAIL mode **Auditors will check to ensure this is turned on.**

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
22	**TAPE DATA SET PROTECTION IS ???????**	
	• Specifies that RACF is to protect the dates on tape.	• Turn on tape dataset protection. • If you have a tape management software and that security is fully defined with RACF this may be off. **Auditors will check to ensure this is turned on. See notes above and may have to describe for Auditors based on customer.**
23	**SECURITY RETENTION PERIOD IN EFFECT IS ?? DAYS**	
	• **RETPD(***nnnnn***)** Specifies the default RACF security retention period for tape data sets.	• Don't worry about retention period if you use tape management software. **Auditors usually don't check this.**
24	**ERASE-ON-SCRATCH IS INACTIVE**	
	• ERASE-ON-SCRATCH--- Specifies whether scratching a disk dataset causes zeroes to be written over the data before the disk space is freed up, 4 options: Not active Active for all datasets Active for datasets with a specified security level or higher For datasets whose RACF profiles have the "ERASE" flag turned on.	• Activate as required in your environment • The Security Technical Implementation Guide (STIG) says to activate this for all datasets. **More and more Auditors will check to ensure this is turned on.**
25	**SINGLE LEVEL NAMES NOT ALLOWED**	
	PREFIX(*prefix***) -** Specifies the PREFIX that RACF should append to datasets with only a single qualifier. Should not be in use any more	• Set single level prefix to suit your taste, or standards. • Should probably not be in use any more **Auditors will not usually check this.**
26	**LIST OF GROUPS ACCESS CHECKING IS INACTIVE**	
	• Specifies that a user's authority to access define a resource is not based only on the authority of the user's current connect group; access is based on the authority of any group to which the user is connected.	• Activate LIST-OF-GROUPS **Auditors will check to ensure this is turned on.**
27	**INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED**	
	• INACTIVE USERIDS--- Specifies the number of days of inactivity after which a USERID will be automatically revoked • If you specify INACTIVE, INITSTATS must be in effect. •	• Revoke inactive USERIDS after some standard number of days **Auditors will check to that there is some value defined.**
28	**NO DATA SET MODELLING BEING DONE**	
	• MODELLING (USER, GROUP, GDG) Specifies that mode dataset profiles will be used to fill in the permit lists of USER, GROUP, or GDG DATASET profiles •	• Leave modelling turned off **Auditors will usually not check this.**

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
29	PASSWORD PROCESSING OPTIONS: THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES PASSWORD CHANGE INTERVAL IS 254 DAYS. PASSWORD MINIMUM CHANGE INTERVAL IS 2 DAYS. MIXED CASE PASSWORD SUPPORT IS IN EFFECT. SPECIAL CHARACTERS ARE ALLOWED. 13 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED. AFTER 4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE REVOKED. PASSWORD EXPIRATION WARNING LEVEL IS 186 DAYS. INSTALLATION PASSWORD SYNTAX RULES: RULE 1 LENGTH(4:5) LLLLL RULE 2 LENGTH(5) AAAAA RULE 3 LENGTH(6:8) LLLLLLLL RULE 4 LENGTH(6:8) NNNNNNNN RULE 5 LENGTH(6:8) AAAAAAAA LEGEND: A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-SPECIAL x-MIXEDALL	**Auditors will check various options to validate these items.** **They may want to review the customers security standards or use the STIG controls.** **More and more they want at least 8 characters, mixed case for passwords.** **KDFAES should be implemented.** **Password history should be some number** **Minchange should be at lease 1 day.** **There should be a password interval.**
	PASSWORD OPTIONS **Algorithm -** Specifies whether KDFAES or the legacy algorithm is used **Interval** – Specifies the number of days before a user needs to change their password or password phrase **Minimum change interval** – Number of days before one can change their password. **Mixed case password** – Specifies whether RACF is to allow lower and upper case passwords **Special Characters** – Specifies whether the additional special characters are allowed **Password history** - Number of recently used passwords (up to 32) maintained in each user profile (to prevent password re-use) **Number of consecutive unsuccessful** - Number of bad passwords in a row which will cause RACF to revoke a USERID **Expiration warning level** -- Number of days before a password expires that a user is warned **Syntax Rules** - Length and content rules **Revoke** - Specifies the number of consecutive incorrect password attempts RACF allows before it revokes the user ID on the next incorrect attempt.	Should be using KDFAES Set password change interval according to business requirements. Minimum change is usually set to at least 1 day. Set based on business requirements. Specifies additional characters as needed by business requirements Set based on business needs and other parameters in the password option. Usually recommend 10. Revoke USERIDS after 3 unsuccessful passwords Set password expiration level to meet business requirements Set syntax rules to include at least 1 number and at least 1 letter (alphanumberic) with a length of 8. Consider using MFA or password phrases Set number based on business requirements.

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
30	**DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.** **DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.**	
	• Specifies the passwords that the operator is to use to respond to requests to approve RVARY command processing, where *switch-pw* is the response to a request to switch RACF databases or change the operating mode of RACF, and *status-pw* is the response to a request to change RACF or database status from ACTIVE to INACTIVE or from INACTIVE to ACTIVE.	• Provide RVARY passwords, change on a regular basis and test **Auditors will check to ensure this is not the default.**
31	**MULTI LEVEL SECURITY**	
	• Discretionary Access Control (DAC) is a method of restricting access to resources (such as datasets or transactions) based on the identity of users or groups to which the users belong. DAC protects all system resources from unauthorized access down to a single user. A user who does not have permission to access a resource can only be granted this permission by the resource's owner. It's up to the discretion of this owner to specify access. Their possibility to pass on access is not restricted in any way. • Mandatory Access Control (MAC) is a method of restricting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity. • You define the sensitivity of the resource by means of a label. This label indicates the level or classification of the information (for example, Restricted, Confidential, or Internal). Within that level, you define the category to which the information belongs (such as Personnel or Research). Users can access only the information in a resource to which their security labels entitle them. If the user's security label does not have enough authority, the user cannot access the information in the resource. **MLACTIVE and NOMLACTIVE** - Use the MLACTIVE and NOMLACTIVE options to control whether security labels are required for certain resources. **MLFSOBJ** - Use the MLFSOBJ option to control whether security labels are required for z/OS UNIX files and directories **MLIPCOBJ** - Use the MLIPCOBJ option to control whether security labels are required for interprocess communication. **MLNAMES and NOMLNAMES** - Use the MLNAMES and NOMLNAMES options to control whether the name-hiding function is in effect. **MLQUIET and NOMLQUIET** - Use the MLQUIET and NOMLQUIET options to control whether the system is in a tranquil state. When the MLSTABLE option is active, authorized users cannot make changes to security labels or change the security labels associated with resources until the security administrator sets the MLQUIET option. **MLS and NOMLS** - Use the MLS and NOMLS options to control whether users who do not have the write-down privilege can write down. **MLSTABLE and NOMLSTABLE** - These options control whether authorized users can make changes to security labels or change the security labels associated with resources while the system is not quiesced. **SECLABELAUDIT and NOSECLABELAUDIT** - You can specify auditing options for a specific security label. You specify these options in the profile in the SECLABEL class that defines the security label. **SECLABELCONTROL and NOSECLABELCONTROL** - These options control whether users other than those with the RACF SPECIAL attribute can make changes to security labels and change the security labels associated with resources. **SECLBYSYSTEM and NOSECLBYSYSTEM** - Use these options to control activation of security labels on a system image basis in a sysplex	• Leave inactive • Unless you have a need to implement. **Auditors will usually not check the settings in this area.**

	SETR EXPLANATION	WHAT SETTING AUDITORS CHECK
34	**GENERIC OWNER ONLY IS NOT IN EFFECT**	
	• GENERICOWNER--- Used with CLAUTH authority to restrict undercutting ("undercutting is the creation of a more specific rule. This has the effect of bypassing the original rule for any resource which matches the more specific rule. •	• If needed for security administration decentralization one may consider turning this on. **Auditors will usually not check the settings in this area.**
40	**CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT**	
	• CATDSNS – Requires all datasets be cataloged, this includes temporary datasets. This might have a negative impact on RACF and system performance because RACF must verify that data sets are cataloged before it allows them to be opened.	• Default is not to activate - Leave the default **Auditors will usually not check the settings in this area.**
41	**USER-ID FOR JES NJEUSERID IS ????????**	
	• Default userid for undefined NJE jobs • Defaulty is ???????? •	• Leave the default **Auditors will check to ensure this is turned on.**
42	**USER-ID FOR JES UNDEFINEDUSER IS ++++++++**	
	• Defines the userid for undefined local jobs • Default is ++++++++ •	• Leave the default **Auditors will check to ensure this is turned on.**
43	**PARTNER LU VERIFICATION SESSION KEY INTERVAL MAXIMUM/DEFAULT IS 30 DAYS**	
	• SESSIONKEY INTERVAL--- Default number of days a session key for APPC is valid •	• Leave the default **Auditors will usually not check the settings in this area.**
44	**APPLAUDIT IS NOT IN EFFECT**	
	• APPLAUDIT - Specifies that auditing of APPC transactions on your system.	• Leave the default • **SYSTEM AUDITOR to change** • **ROAUDIT to view** **Auditors will usually not check the settings in this area.**
45	**ADDCREATOR IS IN EFFECT**	
	• ADDCREATOR--- ADDCREATOR Applies when someone creates a new dataset or resource rule. It automatically permits the USERID creating the rule with ALTER access. •	• ADDCREATOR IS NOT IN EFFCT should be set **Auditors will check to ensure this is turned on.**
46	**KERBLVL = 0**	
	• KERBLVL – specifies the level of key encryption •	OBSOLETE
51	**PRIMARY LANGUAGE DEFAULT : ENU** **SECONDARY LANGUAGE DEFAULT : ENU**	
	• PRIMARY AND SECONDARY LANGUAGES--- Specifies the system-wide defaults for national languages (such as American English or Japanese) to be used on your system. •	• Leave as default **Auditors will usually not check the settings in this area.**

	DSMON Report
Area	**Comment**
System Report	Identification number of the processor complex Model number of the processor complex Name, version, and release number of the operating system System residence volume System identifier used by the System Management Facilities RACF version and release number and whether RACF is active You can use the system report to verify that the system has the expected hardware and software. In addition, you can verify the status of RACF. **Auditors will look to see if on a supported release of z/OS**
Program Properties Table	The program properties table report lists all the programs in the program properties table (PPT). The report also indicates whether each program is authorized to bypass password protection and whether it runs in a system key. The programs shown in this report may be able to bypass password protection for password protected data sets and thus also bypass all RACF protection for RACF-protected resources. You can use the program properties table report to verify that only those programs that should be authorized to bypass password protection are, in fact, able to do so. Such programs are normally communication and database control programs, or other system control programs. You can also verify that only those programs that must run in a system key are authorized to do so. **PROGRAM BYPASS** ISTINM01 YES – IBM default IEEMB860 YES – IBM default IEAVTDSV YES – IBM default IGDSSI01 YES – IBM default COFMINIT YES – IBM default COFMISDO YES – IBM default IOSVROUT YES – IBM default ITTTRCWR YES – IBM default EPWINIT YES – IBM default **Auditors will look to see which programs bypass security**
Authorized Caller Table	The RACF authorized caller table report lists the names of all programs in the RACF authorized caller table. The report also indicates whether each program is authorized to issue a VERIFY (RACINIT) request (which performs user verification) or a LIST (RACLIST) request (which loads profiles into main storage), or both. **Auditors will look to see if this is empty.**
RACF Exits	The RACF exits report lists the names of all the installation-defined RACF exit routines and specifies the size of each exit routine module. **Auditors will check to see if anything is in here. If there is something it needs to be investigated.**
Users	This lists users that are RACF SPECIAL, OPERATIONS, AUDITOR, ROAUDITOR, or GROUP SPECIAL, OPERATIONS, and AUDITOR. It will also list users that are revoked. **Auditors will look to see some of the following:** • **Is IBMUSER revoked?** • **Review the number of SPECIAL, OPERATIONS, AUDITOR, ROAUDITOR in relation to total number of users in the environment** • **Review the number of revoked users and understand business reason as to why they still exist on the system.**
Group Tree	The group tree report lists all subgroups for the SYS1 group and continues to list subgroups for those subgroups on down the group tree. **Auditors will review to see if any groups are owned by users.**
RACF Class Descriptor Table	The class descriptor table report lists class name and status for all general resource classes in the class descriptor table, including information about auditing activity, statistics, the activity of OPERATIONS users, and the universal access authority (UACC). **Auditors will review the following:** • **Ensure auditing is turned on for every class** • **Ensure there is an owner for each class** • **Review the default UACC** • **Review the OPERATIONS allowed to determine if it has been changed from a default or added to a user defined class.**

RACF Global Access Table	The global access checking table report lists all entries in the global access checking table. Each entry consists of a resource name and its associated global access checking authority level. **Auditors will review the following:** • **Are classes active with no entries** • **Review entries that are defined to determine if they allow more access.**
Started Procedures	The started procedures table report lists each entry in the started procedures table. Each entry contains the procedure name, user identification, the group name associated with the procedure, the privileged status, and the trusted status. Privileged started tasks – The PRIVILEGED attribute allows the started task to pass most authorization checking. No installation exits are called, no SMF records are generated, and no statistics are updated. Trusted started tasks – The TRUSTED attribute allows the started task to pass most authorization checking. No installation exits are called, SMF records are generated. **Auditors will look review the following:** • **There should be NO entries of YES under the PRIVILEGE column** • **Question all entries with YES in TRUSTED column** • **Make sure there are USERIDs are defined for the started task** • **Make sure the USERIDs are RACF 'PROTECTED'** • **Review the '**' entry to determine what access that is has and how it is defined.** •
Selected User Attribute report	The selected data sets report lists all the data sets, including the RACF database or databases, that meet one or more of the selection criteria that DSMON uses. For each selected data set, the report specifies the serial number of the volume on which the data set resides, the selection criterion, whether the data set is RACF-indicated or RACF-protected, and the universal access authority (UACC) for the data set. If a data set or RACF database meets more than one selection criterion, there is a separate entry for each criterion. **Auditors will look review the following:** • **Make sure no libraries have a UACC other than NONE** • **Make sure all libraries are protected** • **Question libraries that have a NM (Not Mounted)** • **Question the libraries that have discrete data set profiles** • **Question libraries that have a NF (Not Found)** • **Question libraries that have NC (Not Cataloged)** • **May ask for access lists for some specific libraries**

Join the Conversation!

Unlike professional accountants who can rely on the long standing rubric of Generally Accepted Accounting Practices (GAAP) as a basis to measure their actions and client processes, there is no such a standard for z/OS Security professionals to follow. The z Exchange seeks to resolve this void and address the z/OS skills challenge head on by opening up to our community a conversation that we hope will culminate in a first ever statement of Generally Accepted Security Practices (GASP) for z/OS.

To begin the process, we will rely on the experience and insights of Julie Bergh. Well known within z/OS security circles, with well over 20 years of hands-on experience in applying z/OS security solutions, she has graciously stepped up to share her knowledge and take the first shot in this Version 1 of Generally Accepted Security Practices. This is her work and is presented to encourage your contribution to what we hope will be an ongoing professional and productive conversation.

Please send your thoughts, contributions, additions, corrections, etc. to jms@newera.com

This eBook is published by
The z Exchange
https://zexchange.info

NewEra Software, Inc.
is the proud sponsor of
The z Exchange
https://www.newera-info.com