Ford Motor Company AuditStar Procedures			
		Type **Procedure**	
Subject **AuditStar Administration**		Effective Date **08/17/2006** **Reviewed on:** **08/2007**	
Distribution **Unlimited**	Issued By **TechStar International**	Approvals	Next Review

AuditStar

The purpose of this documentation is to provide procedures for the setup and operation of ***AuditStar***. These procedures include the following sections:

Copyright Information

AuditStar System Reporting

1. Overview

1.1 Description

AuditStar performs a thorough audit on IBM mainframes running zOS and RACF by providing a fully automated security scorecard that reports deviations from installation-specific security standards and IBM best practices. The standards cover all the important security system parameters and privileges.

AuditStar captures information about access protection and system integrity for each MVS Image on the mainframe. Periodically, it sends the information to the ***AuditStar*** server for storage and evaluation. ***AuditStar*** detects discrepancies and reports them to the user for review.

AuditStar runs once a day. All reports are generated daily, as well, but other frequencies are possible. Some reports may be required only on a weekly basis.

1.1.1 Definitions

- MVS – The IBM Mainframe Business Operating System, now called zOS.
- RACF – Resource Access Control Facility for IBM

1.2 Responsibilities

AuditStar runs automatically to generate its daily reports. The specified Security Department Analyst, who initiates any investigation necessary, reviews the reports. Other individuals may be allowed to review reports as well (managers, etc.) to track trends within their areas of responsibility.

1.3 Concepts

1.3.1 Clusters and Systems

AuditStar reports items at two different levels: Cluster level and System level.

An ***AuditStar*** cluster is all MVS images sharing a single RACF database. All user privileges and profiles defined in the RACF database are the same in every system sharing the database. ***AuditStar*** reports on these items at the cluster level only. Clusters may also be known as a RACF Facility

Many RACF parameters and tables can have different settings for each system even when the systems share the same RACF database. If a RACF item can be set differently for each system, ***AuditStar*** reports that item at the system level. This is true even when MVS or RACF is set to propagate settings automatically from system to system. ***AuditStar*** also reports on MVS settings related to security and integrity at the system level, including IPL parameters, SVCs, I/O appendages and other system settings.

1.3.2 Standards

The standards ***AuditStar*** uses for its comparisons have been customized based on Ford Motor Company policies and IBM best practices. This includes all RACF and MVS resource protection information, user privileges, RACF and System tables, and all system parameters related to operational integrity. The standards also include information about sensitive programs and subsystems. Standards will be discussed in greater detail later in this document.

1.3.3 Discrepancies

AuditStar triggers a discrepancy when it detects a security parameter or privilege on the system that does not match the standard as stored in the database. The program reports the discrepancies to the administrator who can then review them and resolve them. Discrepancies will be discussed in greater detail later in this document.

1.3.4 Reports

The routine daily audits performed by ***AuditStar*** result in an automatic deviation analysis. The analysis results in a series of summary and detailed discrepancy reports that list all items that do not meet standards, and all discrepancies that have been resolved. The administrator can review the reports and take any actions that are necessary. The reports allow the administrator to spot trends as well as individual discrepancies so that management can consider changes to information security systems.

All reports are presented online for viewing, but may be copied to an Excel spreadsheet format and printed for later analysis.

1.3.5 Concerns

A concern is a discrepancy that may require corrective action of some type, such as human intervention or a policy decision.

1.3.6 Forms

The screens and dialog boxes you use to enter data, create filters, etc., in ***AuditStar*** are known as forms.

1.4 Requirements

In order for ***AuditStar*** to run, you must have valid licenses for two other software products:

- ***AuditStar*** uses an ***Oracle*** database, which must be licensed (from Oracle), and
- ***AuditStar*** extracts data from RACF and MVS by using *either*
  - ***AuditStar zExtract*** (from TechStar International) *or*
  - ***Consul zAudit*** (from Consul Risk Management)

You must also have the necessary permissions and have the Client version of AuditStar (GUI portion) installed on your workstation.

2. Using AuditStar

2.1 Monitoring Discrepancies

A standard is the value ***AuditStar*** expects to find on the system for an item that is being monitored. ***AuditStar*** generates discrepancies when data on the system does not match the standards for the system.

2.1.1 Discrepancy Status

A one-character status is associated with each discrepancy. The value changes when the discrepancy is resolved. Allowable values are shown below.

Status	Definition	Explanation
A	Accepted	The discrepancy was accepted, and the standard has been updated to reflect the current value.
C	Closed	The discrepancy was closed.
N	Not in Standards	A current value has been detected that does not exist in the standards. There is no value with which to compare it.
O	Open	A standard exists on which to base this comparison. The current value and the standard do not match.
Q	Required	A value that is in the standard has not been found in the current data. A parameter is missing.
M	Removed	The standard has been removed or deleted (this is often the method chosen to resolve a “Required” deficiency).

2.1.2 Resolving Discrepancies (Overview)

Before a discrepancy may be resolved, the Analyst must investigate it. This may involve finding out who entered the information that generated the discrepancy and determining the reason why the entry was made. If the entry is the result of a simple error, the discrepancy can be resolved readily. If further investigation is necessary, the Analyst will contact the appropriate manager to determine how the discrepancy should be resolved.

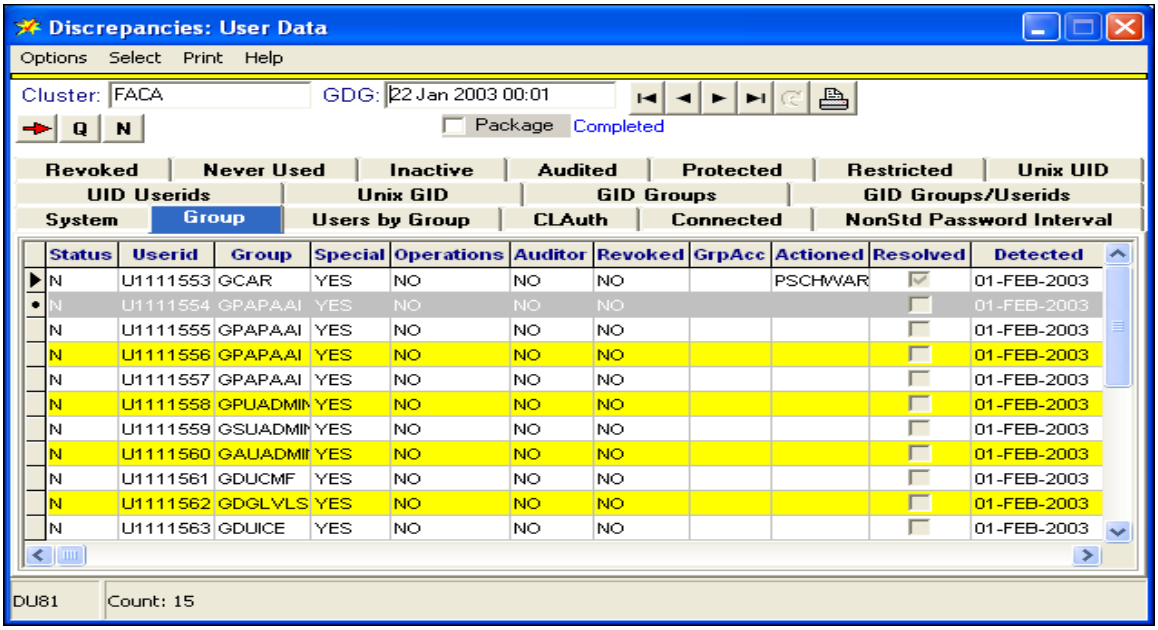
A discrepancy is considered resolved when its status is changed from N, O, or Q to A, C or M (see the list above). If you have the correct level of authority, you may resolve a discrepancy by applying one of the following actions from one of the *Discrepancy* screens:

- Accept – change the standard to match the current value. This adds the standard to the database or updates the existing standard so the value on the mainframe exactly matches the standard stored in the ***AuditStar*** database.
- Remove – delete the standard from the system. In some cases a standard stored in the database will not be found on the system. For example, a user ID may have been assigned

the Group Special privilege. Later, that privilege is removed from the user ID either because the employee has left the company or because their role has changed within the company. In this case, the privilege needs to be removed from the ***AuditStar*** standard.

- Correct the setting on the system (reset the standard). A discrepancy can be resolved by changing the setting on the system to match the value in the ***AuditStar*** standards. For example, if a user is not supposed to have System Special privileges as reflected in the ***AuditStar*** standards, but in fact does have that privilege in the RACF database, the discrepancy can be resolved by removing that privilege from the user in the RACF database.

2.1.3 The Discrepancies List Screen



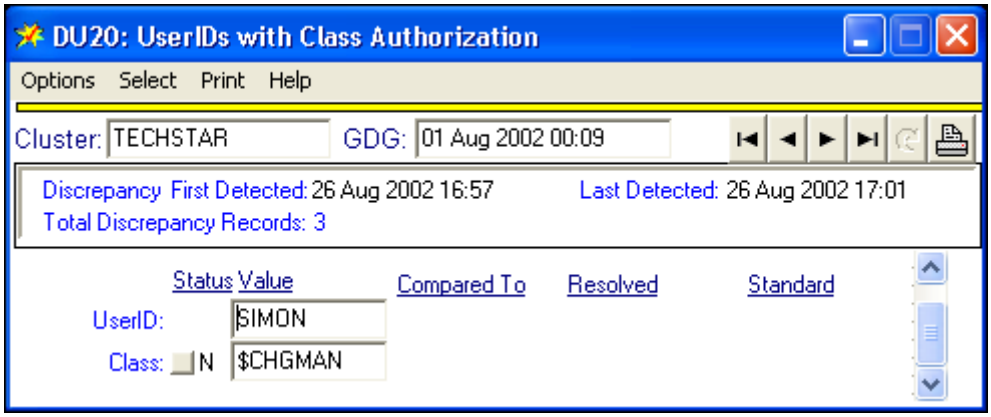
The list screen provides a table of all discrepancies for easy scanning. There are special fields and features available on this screen.

Field or Feature	Description
Actioned (Field)	Identifies the last user ID to resolve or otherwise act on the discrepancy in AuditStar.
Resolved (Field)	Checked if the discrepancy has been resolved or actioned in AuditStar.
First Detected (Field)	Shows the date AuditStar detected the discrepancy. **Note:** You may toggle this information on or off by using the "Discrepancies: Show First Detected" menu option on the main screen.
Double-Click for Detail (Feature)	You may double-click on any record on the *Discrepancy List* screen, and the *Discrepancy Detail* screen will open to that record.

You may resolve discrepancies on this screen by selecting any one of four buttons:

Button	Command	Result
Right arrow 	Resolve Selected Discrepancies	The discrepancies you have selected (by clicking them) will be resolved. Type Q discrepancies will be removed from the standards; All others will be accepted into the standards.
Q 	Resolve Q Discrepancies	All type Q discrepancies will be removed from the standards. No filtration or selection will apply.
N 	Resolve N Discrepancies	All type N discrepancies will be added to the standards. No filtration or selection will apply.
Sigma (summation sign) 	AutoResolve or Mass Resolve Discrepancies	AuditStar will resolve all discrepancies that may currently be viewed based on the filtering applied. Type Q discrepancies will be deleted from the standards. All others will be accepted. **Note:** You may toggle this option on or off in the Application Setup menu.

2.1.4 The Discrepancies Detail Screen

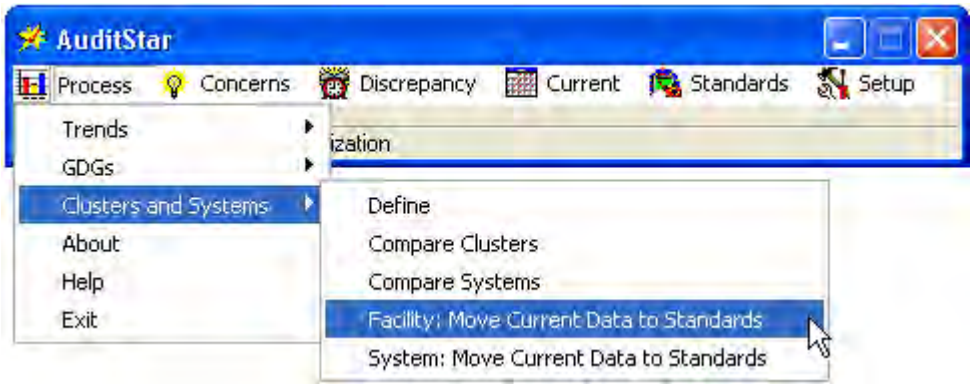


The detail screen provides details for each discrepancy, including the standard that applied and the current standard (in case the standard has changed). This screen provides more control over how a discrepancy is resolved than is provided by the list screen.

To resolve the discrepancy at the detailed level, click on the button in the Status column next to the item you want to change. A pop-up menu opens displaying your choices. Options not available to you will be grayed out. Click the option you want and ***AuditStar*** resolves the discrepancy.

Important: Additional information about resolving discrepancies will be discussed in greater detail in Section 6.4 Examining Discrepancy Details.

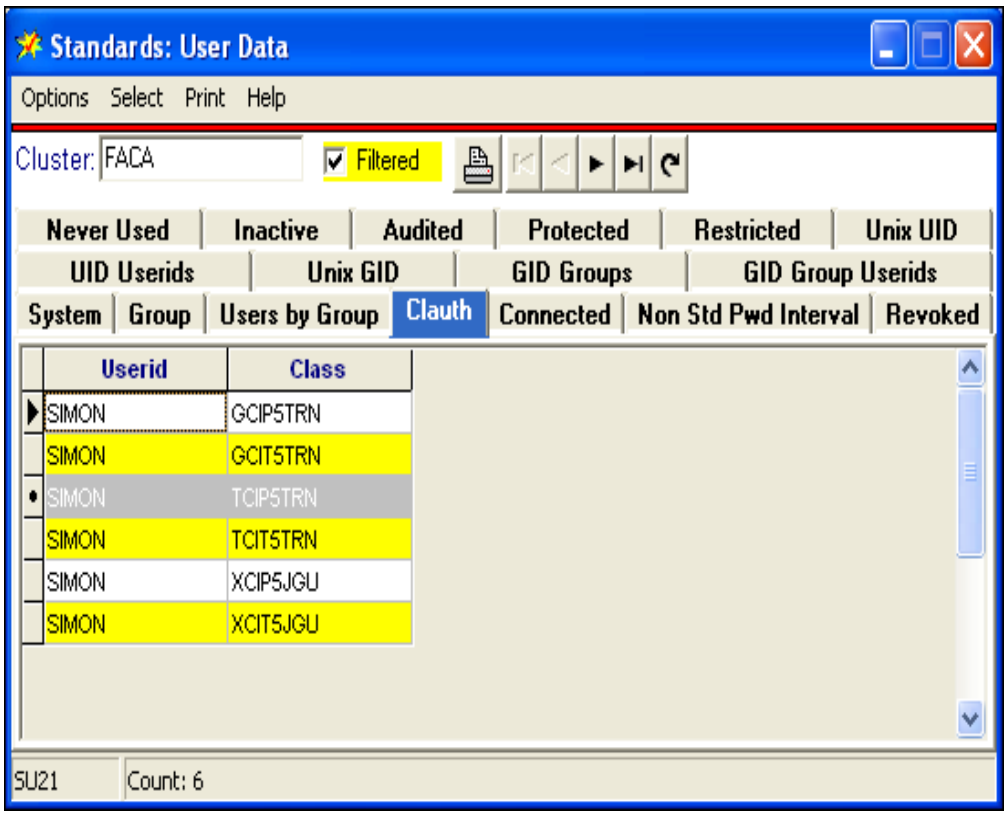
2.2 Standards



You can use a variety of ways to create or revise standards to be applied by ***AuditStar***:

- You can resolve discrepancies, as discussed above, and automatically generate changes to the standards
- You can move the current data from one or more tables for any cluster or system to the standards. This can be done from any current data screen or from the “Process>Clusters” and “Process>Systems” submenus on the ***AuditStar*** screen
- You may directly enter and edit standards on the *Standards* screen

2.2.1 Updating the Standards



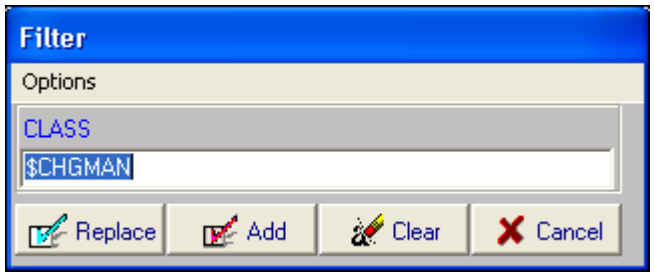
You may edit the standards directly by turning on the Edit Mode option on the *Standards* screen. This opens an extended navigation bar that lets you edit, add or delete standards.

You may also update the standards by using the menus on any current data screen, or from the Cluster and System options on the ***AuditStar*** main screen.

Furthermore, you may update the standards by using the "Cluster and System to Standards" option from the main menu.

2.3 Filtering Data

You can restrict or specify the information you want included in an audit (and the resultant report) by creating a filter for any given parameter.

Step	Action
1	Select a parameter and right-click on it (or press F3). Result: The *Filter Options* form opens.
2	 On the form, enter the criterion you want to apply. Click "Add." Result: The criterion becomes the filter for the parameter you selected.
3	If a filter has already been established, you may add criteria to it by following the steps above and pressing "Add" (see **Compound Filters**, below). Result: The criterion is added. If you want to replace the existing filter, follow the steps, but select "Replace." Result: The existing criteria are replaced with the new one you have chosen.

By default, the filter will choose all data that starts with the value you entered, and the report will be filtered accordingly.

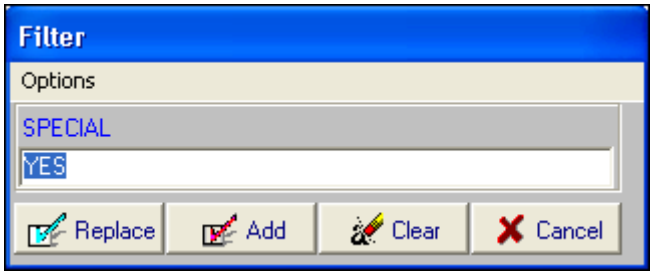
You may also manage filters by using the "Options" menu on the *Filter Options* form. You can do the following:

- Clear a Filter = click the "Clear" button, or click the filter check box if it appears. All filters on the record you are viewing will be cleared.
- Use Wild Card Characters = use the underline character "_" and the percent sign "%" to create more complex filters. For example, a filter like `M_W` will cause ***AuditStar*** to find any data with a first character of M, and third character of W, and any second character. A filter like `A%` will find any data beginning with A.
- Use Numeric Filters = create the filtering condition by using >, <, and = to determine the data you want to audit. A filter like >=3 will cause ***AuditStar*** to find any data with a value greater than or equal to 3.

- Use Not Null Filters = use a filter condition `NOT NULL` to find records where a specific field is not blank. The SQL standard is that an empty string is not the same as a null value. The NOT NULL filter may find some records where a field value appears blank but actually contains a blank string.

2.3.1 Compound Filters

If a filter already exists, you can create a compound filter by adding a criterion to the filter and using `OR` or `AND` in front of the additional criterion. This will cause ***AuditStar*** to find data that matches either one criterion or the other, or both criteria.



If a filter already exists for the records you are viewing and you do not use `OR` or `AND`, the new condition will replace the old one.

2.3.2 User or Group Information

On any form that contains User ID data, you can get the installation data about the user by using the “Options” menu or by entering `Ctrl U`.

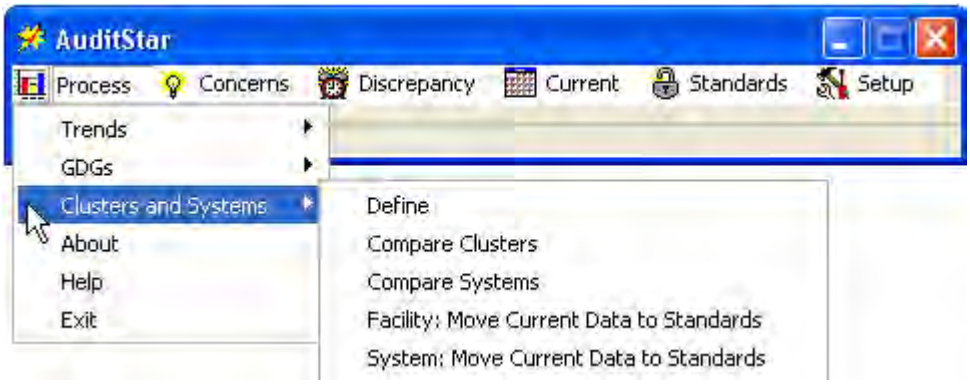
On any form containing Group data, you can get the installation data by using the “Options” menu or entering `Ctrl G`.

3. Comparison Reports

3.1 Comparing Clusters and Systems

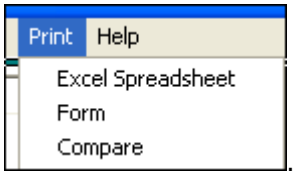
You may make *ad hoc* comparisons of data for any table. This includes comparisons of values in different generations (old and new values) of a single table for a selected System, or the values in a table on one system with that same table on another system.

To perform comparisons, choose one of the following menu options from the Process menu on the ***AuditStar*** main screen:

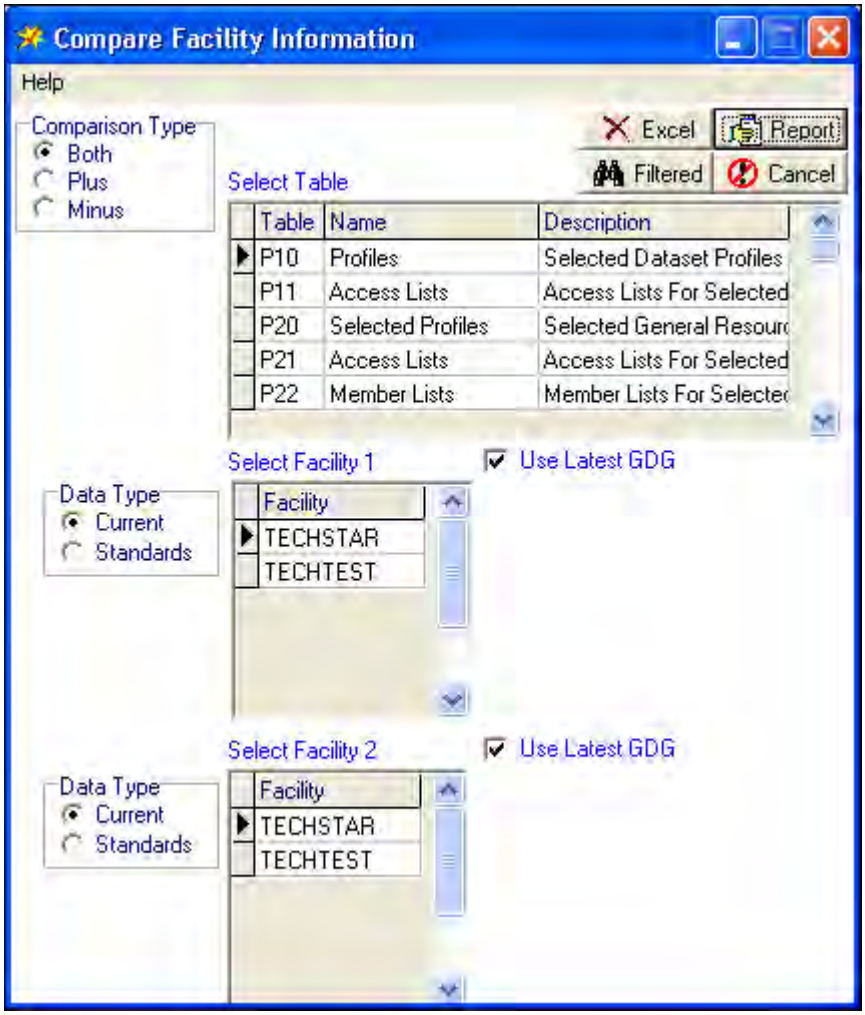


- Select “Compare Clusters” to access and compare cluster level information
- Select “Compare Systems” to access and compare system level information

Note: You can also select these menu options from the “Print” menu of many screens



3.2 Comparison Options



Selecting one of the comparison menu items from the main window will cause the appropriate *Compare* window to open. ***AuditStar*** will present the discrepancies or items it finds by identifying each item with a plus sign or a minus. ***AuditStar*** identifies items that are present in your first cluster or system selection but not in your second selection with a plus (+); it identifies those present in your second selection but not in your first selection with a minus (-).

In the *Compare* window you may choose the type of comparison you want to run (by selecting the radio button for plus comparisons only, minus comparisons only, or both). From list boxes, you choose the table name you want to audit, plus the two systems or facilities to be compared. Radio buttons also identify the type of data you want to audit (current values or standard values).

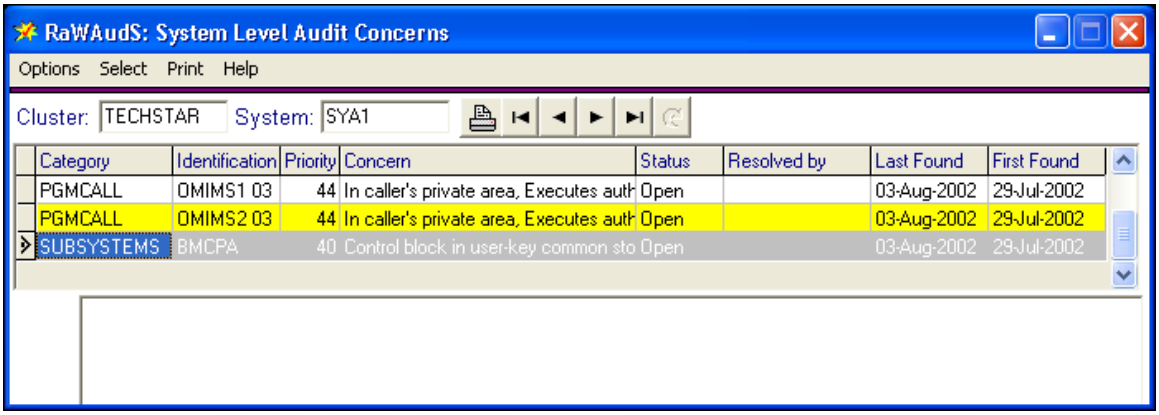
You can compare current values to current values or standard values to standard values on the identified table in different systems, or current values to standard values on the identified table in the same system.

4. Automated Audits

The audits run by ***AuditStar*** generate discrepancies, some of which denote concerns. There are four categories of concerns:

1. Automated Audit concerns – serious security or system integrity issues that should be analyzed immediately.
2. Self-Audit concerns – audit issues that the administrators have entered so they can be managed and resolved.
3. Warnings – security and system integrity issues that have been flagged as (a) requiring cleanup or (b) being contrary to usual practice. These warnings do not generally pose security threats, but their cleanup may be viewed as bookkeeping issues.
4. RACF Database Usage – the size of the database may become a concern, particularly if it grows very large. Data regarding these concerns are for information purposes only, and are not managed or resolved like other concerns.

You may view and manage concerns from the *RaWAudS: System Level Concerns* screen.



4.1 Resolving Concerns

If you have the proper permissions, you can use the “Options” menu to enter “Edit Mode” to change the status of any concern. You may also use the F2 key for this purpose.

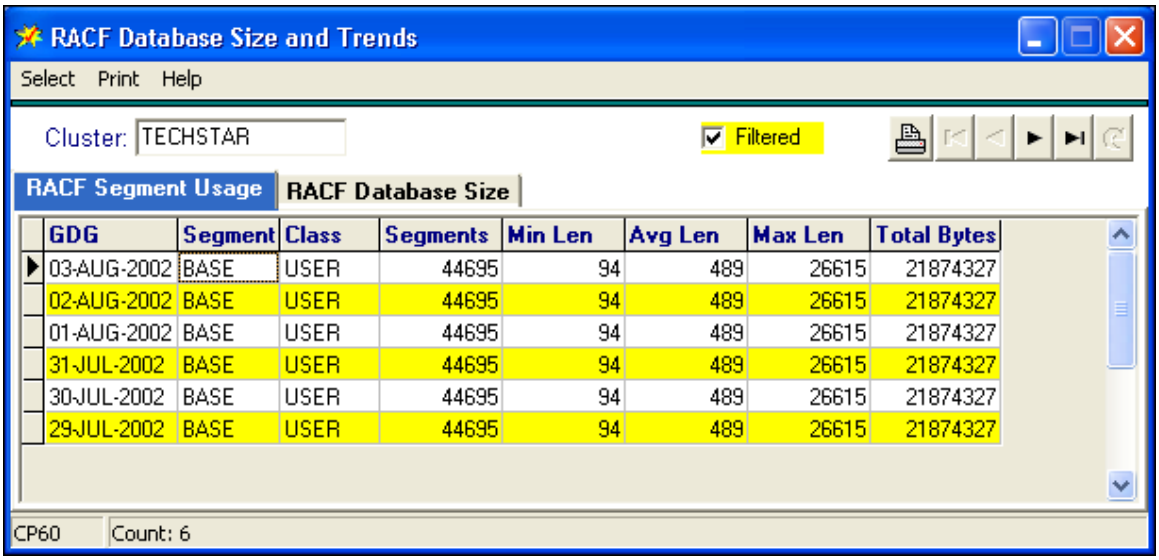
Allowable status designations are shown in the table below:

Status	Description
Closed	The item has been accepted as normal or as an acceptable deviation
Concern	The item has been determined to be a concern, but has not been resolved
Deferred	The item has been noted with resolution deferred to a later date
Open	The item is awaiting determination of status or resolution
Remove	The item will be removed upon the next daily cycle of AuditStar. If the same concern is generated in the future, it will display again.

You may view concerns of varying statuses by changing the filter set on the screen. Right click in the status column to change the filter.

4.2 Database Usage

You may monitor the database usage for Segments and Classes and review usage trends over time on the *RACF Database Size and Trends* screen.



4.3 Shared DASD

There is a special report that lists all shared DASDs by physical device across all systems in the IBM mainframe systemplex. ***AuditStar*** identifies every system that shares that device.

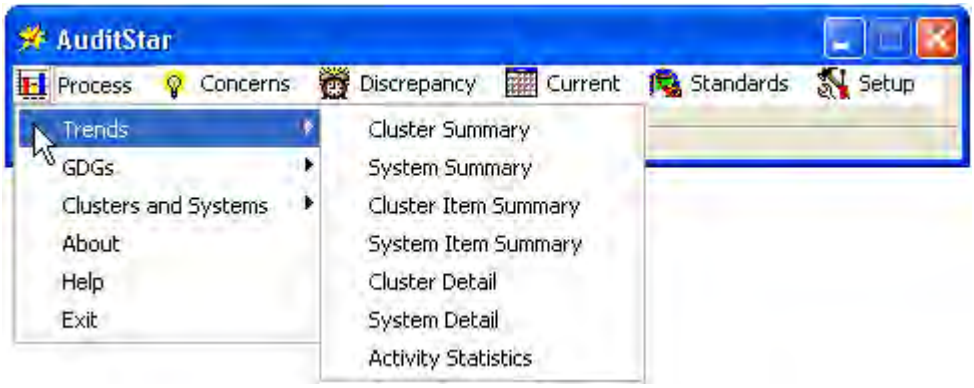
According to standard practice, each physical device uses the same Volume Serial (Volser) on each system. If different systems refer to the same DASD with different Volsers, problems arise. These problems generate warnings in the report. You view the report on the *CG10: Shared DASD* screen.

4.3.1 Definition

- DASD – Direct Access Storage Device, typically a disk drive, but possibly a different electronic device that is accessed in the same manner.

5. Trends

5.1 Trend Options

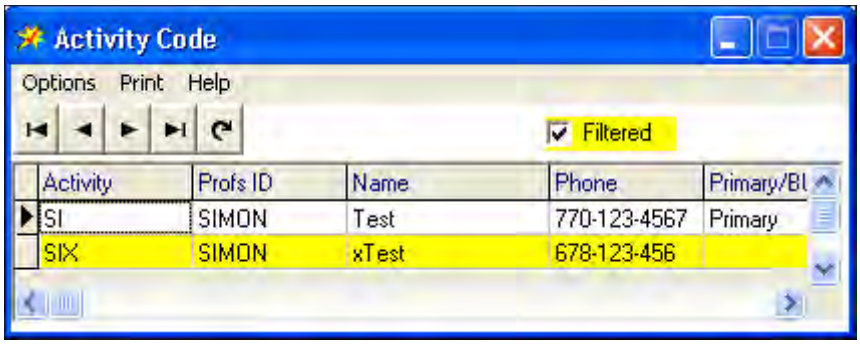


You may access several screens that give you an overall picture of security by selecting the Trends option on the ***AuditStar*** main menu. The menu choices (screens) available to you are shown in the following table.

Option	Description
Cluster Summary	Summary of discrepancies at the Cluster level
System Summary	Summary of discrepancies at the System level
Cluster Item Summary	Trends over time for each Cluster level item
System Item Summary	Trends over time for each System level item
Cluster Detail	Number of open items of each type for a selected Cluster and generation (GDG)
System Detail	Number of open items of each type for a selected System and generation (GDG)
Activity Statistics	Breakdown of discrepancies by user ID activity or prefix for the latest generation (GDG) only. **Note:** This screen lists the number of discrepancies for each Activity in the Activity table; the data may be filtered. You can reach the list of activities by selecting the “Activity Codes” option from the “Setup” menu on the AuditStar main screen.

5.2 Trend Activities

You can edit activities and turn automated e-mail reports on or off from the *Activity Code* screen. Use the “Options” menu or the F2 key to put the data in “Edit” mode.

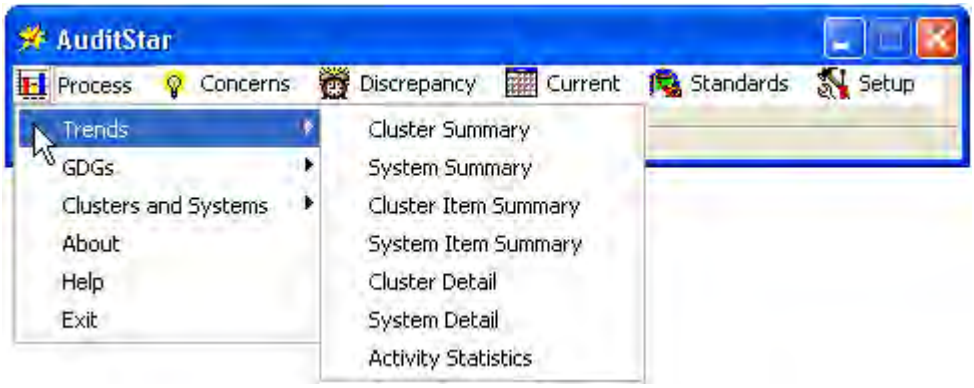

Activity Code
Options
Print
Help
Filtered
Activity
Profs ID
Name
Phone
Primary/Bl
SI
SIMON
Test
770-123-4567
Primary
SIX
SIMON
xTest
678-123-456

6. An AuditStar Workflow

The goal for using ***AuditStar*** is to make certain security standards are not violated, which also means you have to be sure the standards are up to date. ***AuditStar*** will help you do this easily. The information that follows is based on Cluster level information, but will apply equally to System level information.

6.1 Trends

Begin the day by looking at trends for any cluster (or system) you want to monitor. You can do this by selecting `Process > Trends > Cluster Summary` from the main ***AuditStar*** screen.



Other trend options are available if you wish to see something other than the cluster summary. The *Cluster Summary Trends* screen opens.

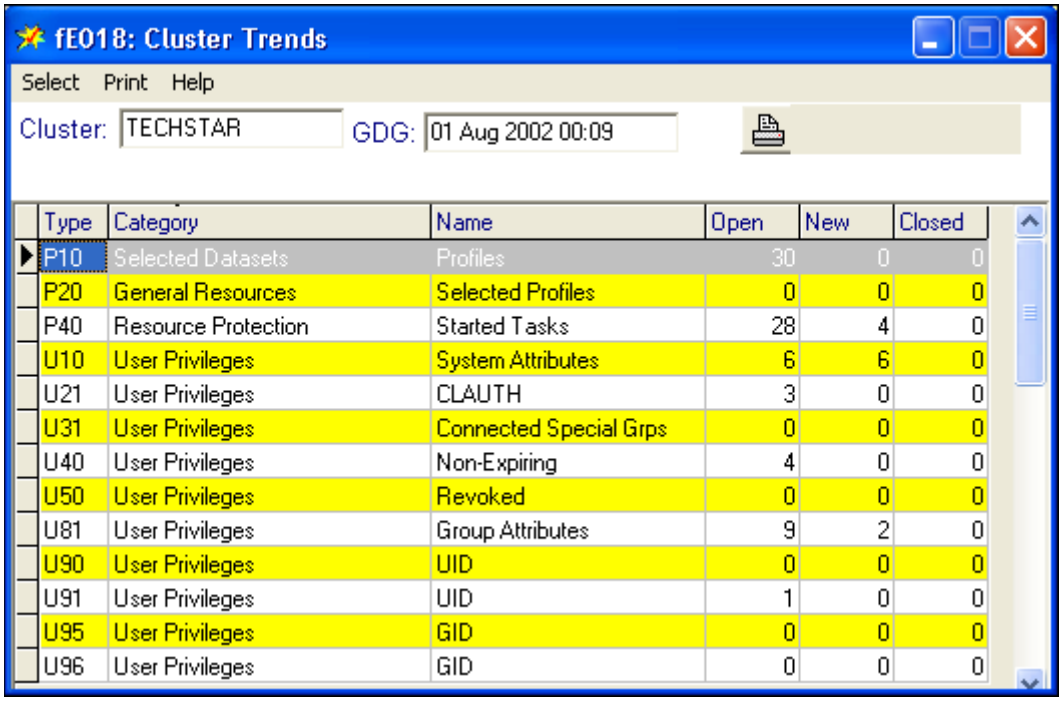
This screen shows a summary of the discrepancy history for the specified cluster, indicates if the data is filtered, and provides a summary by date of the number of open discrepancies and new discrepancies, as well as the number of discrepancies that were closed on that date.

From this screen you may select any of three reports. You can generate a summary report that shows discrepancy trends over time for the single cluster, a composite report that shows the current state of discrepancies for all clusters, or an Excel spreadsheet summarizing this cluster. The spreadsheet offers the advantage that it can be saved and analyzed independently of ***AuditStar***

If you double click on the row for the latest generation of discrepancies for the cluster, you will be able to review discrepancies by type.

6.2 Discrepancies by Type

When you have pinpointed the cluster and generation you want to investigate, double click on the row for that generation on the *Cluster Summary Trends* screen, or select the `Process > Trends > Cluster Item Summary` menu item from the ***AuditStar*** main screen. The *Cluster Trends* screen opens.



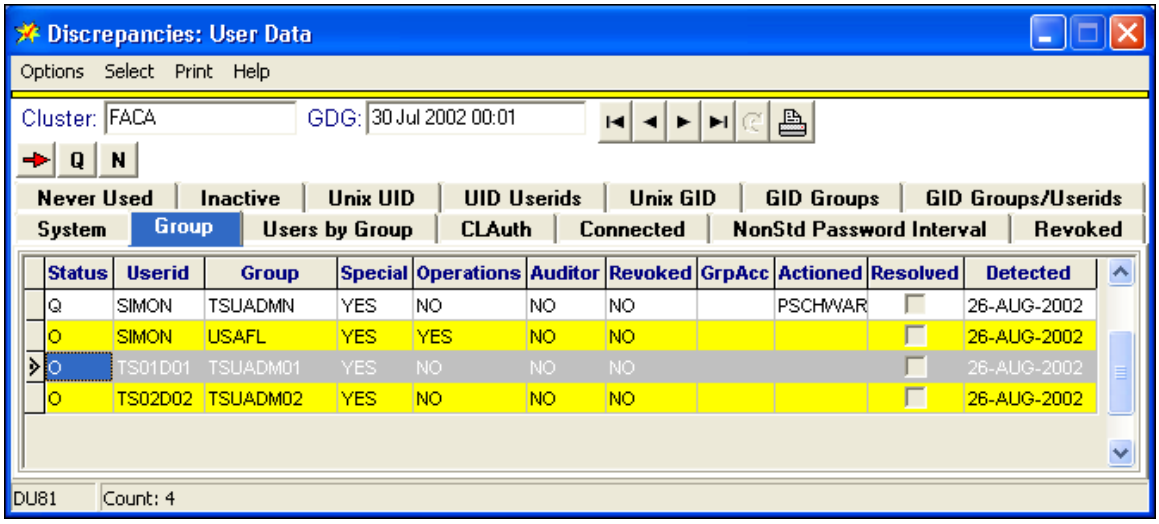
Type	Category	Name	Open	New	Closed
P10	Selected Datasets	Profiles	30	0	0
P20	General Resources	Selected Profiles	0	0	0
P40	Resource Protection	Started Tasks	28	4	0
U10	User Privileges	System Attributes	6	6	0
U21	User Privileges	CLAUTH	3	0	0
U31	User Privileges	Connected Special Grps	0	0	0
U40	User Privileges	Non-Expiring	4	0	0
U50	User Privileges	Revoked	0	0	0
U81	User Privileges	Group Attributes	9	2	0
U90	User Privileges	UID	0	0	0
U91	User Privileges	UID	1	0	0
U95	User Privileges	GID	0	0	0
U96	User Privileges	GID	0	0	0

The *Cluster Trends* detail screen breaks out discrepancies by type and category, and shows the numbers of Open, New, and Closed discrepancies. You may filter the data as you choose to investigate the discrepancies you need to review.

You may investigate each of the discrepancies in detail by double clicking on the row for the specific discrepancy. The *Discrepancies: User Data* list screen opens.

6.3 Examining a List of Discrepancies

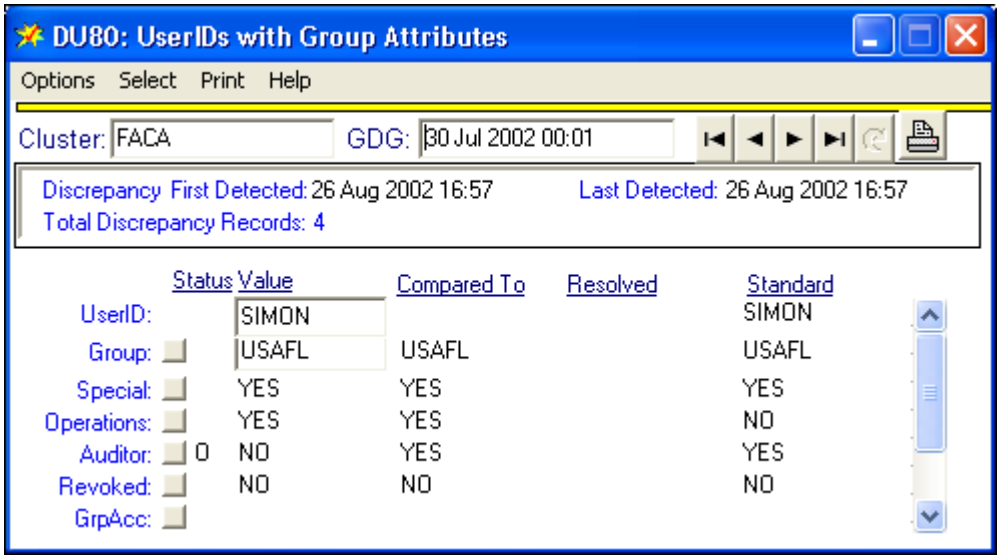
You may double click on a specific item on the *Cluster Trends* screen or select the `Discrepancy > List > User Privileges` menu item from the ***AuditStar*** main screen to open the *Discrepancies: User Data* list screen. Then you may select the tab (e.g., the "Group" tab) denoting the specific kind of data you wish to review.



You may resolve discrepancies directly on this screen or you may review more detailed information on each discrepancy if you wish. Double click on any discrepancy record to go to the *Discrepancy Detail* screen.

6.4 Examining Discrepancy Details

When you open the *Discrepancy Detail* screen, you see user ID information and historical records about the specific discrepancy, including the date it was first detected, the date of the latest occurrence, and the total records for that discrepancy and user. You may resolve the discrepancies as has been explained if you have the correct permissions.



7. Security Department Reviewed Reports

The following reports generated by ***AuditStar*** must be reviewed promptly to determine any actions required. They may then be archived.

7.1 Program Properties Table

<table>
<tr><td>Report Name:</td><td colspan="4">R80: Program Properties Table</td></tr>
<tr><td>Environment:</td><td colspan="4">IBM HOST</td></tr>
<tr><td>Application:</td><td colspan="4">Auditstar</td></tr>
<tr><td>Report Description:</td><td colspan="4">
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Module</td><td>Module name</td><td></td><td>Any changes</td></tr>
<tr><td>Member</td><td>Member name</td><td></td><td>Any changes</td></tr>
<tr><td>Dsname</td><td>Dataset where program exists</td><td>Dsname, or ‘** MODULE NOT FOUND **’ if not located anywhere</td><td>Any changes</td></tr>
<tr><td>Volser</td><td>Volser of dataset</td><td></td><td>Any changes</td></tr>
<tr><td>Profile</td><td>PROGRAM class profile</td><td></td><td>Any changes</td></tr>
<tr><td>Attr1</td><td>Attribute 1</td><td>‘Key xx’, ‘Bypass’ AuthPgm, AuthTSF, AuthCmd</td><td>Any changes</td></tr>
<tr><td>Attr2</td><td>Attribute 2</td><td></td><td>Any changes</td></tr>
<tr><td>Attr3</td><td>Attribute 3</td><td></td><td>Any changes</td></tr>
<tr><td>Attr4</td><td>Attribute 4</td><td></td><td>Any changes</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td colspan="4">There is 1 CR80 record for every module that is inheriting attributes of BYPASS or KEY ‘xx’ from the MVS PPT (Program Properties Table), and any module that has any TSO authorities (from the IKJxx member).
Note that this record requires analysis of both the MVS PPT and all of the existing APF libraries on the system.
Current settings were verified and stored as the standard. Additions, deletions, changes and deviations from standard are automatically reported as discrepancies.</td></tr>
<tr><td>Run Cycle:</td><td colspan="4">Daily - Business Days</td></tr>
<tr><td>Resource:</td><td colspan="4">Automated</td></tr>
<tr><td>Reviewer:</td><td colspan="4">Security Analyst</td></tr>
<tr><td>Media:</td><td colspan="4">Stored Online</td></tr>
<tr><td>Baseline:</td><td colspan="4">Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
</table>

Review Criteria:	Report flags any changes listed in the Monitor Changes column. Some programs require extraordinary privileges not normally permitted by the operating system. The Program Property Table (PPT) contains the names and properties of these special programs. There is one CR80 record for every module that is inheriting attributes of BYPASS or KEY 'xx' from the MVS PPT (Program Properties Table) and any module that has any TSO authorities (from the IKJxx member). Note that this record requires analysis of both the MVS PPT and all of the existing APF libraries on the system. Current settings were verified and stored as the standards. Additions, deletions, changes and deviations from standards are automatically reported as discrepancies. When "** NO MODULE FOUND **" is in the Module field it should be accepted into the standards. If the library is subsequently used to store that module it will then appear as a discrepancy. This let's the security analyst know that a previously deleted authorized module has been reinstalled. In such a case this can indicate a rogue module installation.
Actions:	When problems are found, Security Analystwill investigate and perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.
Action Taker:	Security Analyst
Report Retention:	6 months
Evidence of Review:	AuditStar has an audit trail that keeps track of reviewer, action and dates. Note: This report will be produced **only** when there is a change.

7.2 Modules with Scan Hits

<table>
<tr><td>Report Name:</td><td>090: Modules with Scan Hits (Includes APF (Authorized Program Facility)Modules)</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Member</td><td>Member Name</td><td></td><td>Any change</td></tr>
<tr><td>Dataset Name</td><td>Dataset</td><td></td><td>Any change</td></tr>
<tr><td>Volser</td><td>Volume and Serial (DASD)</td><td></td><td>Any change</td></tr>
<tr><td>Linkedit</td><td>Link Edit</td><td></td><td>Any change</td></tr>
<tr><td>Scan Instructions</td><td>Suspicious Instructions</td><td></td><td>Look for any instructions with scan hits</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>There is 1 C090 record for each Module with a scan hit that is installed on the system</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Any new module with a scan hit that is identified is reported as a discrepancy and must be investigated.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Security Analystar notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
<tr><td>Evidence of Review:</td><td>AuditStar has an audit trail that keeps track of reviewer, action and dates.
Note: This report will be produced only when there is a change.</td></tr>
</table>

7.3 Sensitive Dataset Profiles

<table>
<tr><td>Report Name:</td><td>P10: Sensitive Dataset Profiles</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Default value (reqd)</th><th>Monitored Controls</th></tr>
<tr><td>Class</td><td>Literal ‘DATASET’</td><td></td><td>DATASET</td><td></td></tr>
<tr><td>Profilekey</td><td>Profile key</td><td></td><td></td><td></td></tr>
<tr><td>Profile type</td><td>Discrete or generic</td><td></td><td></td><td>Discrete profiles not permitted</td></tr>
<tr><td>Owner</td><td>Owner</td><td></td><td></td><td>Production datasets may not be owned by nonApplication userids</td></tr>
<tr><td>UACC</td><td>Universal access</td><td></td><td></td><td></td></tr>
<tr><td>Success</td><td>Audit successful access level</td><td></td><td></td><td></td></tr>
<tr><td>Failure</td><td>Audit failed access level</td><td></td><td></td><td></td></tr>
<tr><td>Warning</td><td>Warning mode ?</td><td>Yes, No</td><td></td><td>Warning mode not permitted</td></tr>
<tr><td>Erase</td><td>Erase on delete ?</td><td>Yes, No</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td></td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.</td></tr>
<tr><td>Actions:</td><td>When problems are found, the owner of the dataset will be notified for further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
</table>

Evidence of Review:	AuditStar has an audit trail that keeps track of reviewer, action and dates. Note: This report will be produced **only** when there is a change.

7.4 Supervisor Calls / Extended Service Routers

<table>
<tr><td>Report Name:</td><td colspan="4">O50: Supervisor Calls (SVC) / Extended Service Routers (ESR)</td></tr>
<tr><td>Environment:</td><td colspan="4">IBM HOST</td></tr>
<tr><td>Application:</td><td colspan="4">Auditstar</td></tr>
<tr><td>Report Description:</td><td colspan="4"><table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>SVCno</td><td>SVC number</td><td>N</td><td>Any changes</td></tr>
<tr><td>ESRno</td><td>ESR number</td><td>N,*</td><td>Any changes</td></tr>
<tr><td>Program</td><td>Program name</td><td></td><td>Any changes</td></tr>
<tr><td>Length</td><td>Program length</td><td></td><td>Any changes</td></tr>
</table></td></tr>
<tr><td>Security Controls:</td><td colspan="4">There is 1 CO50 record for the current version of each SVC / ESR installed on the system.

Current SVC/ESRs were verified and stored as the baseline. Additions, deletions, changes and deviations from baseline are automatically reported as discrepancies.</td></tr>
<tr><td>Run Cycle:</td><td colspan="4">Daily – Business Days</td></tr>
<tr><td>Resource:</td><td colspan="4">Automated</td></tr>
<tr><td>Reviewer:</td><td colspan="4">Security Analyst</td></tr>
<tr><td>Media:</td><td colspan="4">Online</td></tr>
<tr><td>Baseline:</td><td colspan="4">Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td colspan="4">Report flags any changes listed in the Monitor Changes column.

SVCs and ESRs are powerful program modules that can be written to bypass security controls. Current SVCs and ESRs are verified for integrity and stored as the standards. Any change can introduce a serious security concern. Additions, deletions, changes and deviations from standards are automatically reported as discrepancies.</td></tr>
<tr><td>Actions:</td><td colspan="4">When problems are found, Security Analysts are notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td colspan="4">Security Analyst</td></tr>
<tr><td>Report Retention:</td><td colspan="4">6 months</td></tr>
<tr><td>Evidence of Review:</td><td colspan="4">AuditStar has an audit trail that keeps track of reviewer, action and dates.

Note: This report will be produced only when there is a change.</td></tr>
</table>

7.5 Program Calls

<table>
<tr><td>Report Name:</td><td>O71: Program Calls</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored Controls</th></tr>
<tr><td>Owner</td><td>Owning Jobname</td><td></td><td>Any change</td></tr>
<tr><td>Ex</td><td>Index into Entry Table</td><td></td><td>Any change</td></tr>
<tr><td>SystemWide</td><td>Systemwide PC?</td><td>Yes, No</td><td>Any change</td></tr>
<tr><td>AuthReq</td><td>Authority Required to use PC?</td><td>Yes, No</td><td>Any change</td></tr>
<tr><td>State</td><td>Execution mode</td><td>SUPERVISOR,PROBLEM</td><td>Any change</td></tr>
<tr><td>Description</td><td>Functional description of program call if known</td><td></td><td>Any change</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>There is 1 CO71 record for each Program Call installed on the system. The program calls are automatically reported.</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standard is stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.
Program Calls can allow calling modules to bypass security controls. All program calls are verified for integrity. Any additions, deletions or updates are reported as discrepancies and must be reviewed.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Technical Services is notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
<tr><td>Evidence of Review:</td><td>AuditStar has an audit trail that keeps track of reviewer, action and dates.
Note: This report will be produced only when is a change.</td></tr>
</table>

7.6 Authorized I/O Appendages

<table>
<tr><td>Report Name:</td><td>O60: Authorized I/O Appendages</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored Controls</th></tr>
<tr><td>ID</td><td>Appendage ID</td><td></td><td>Any change</td></tr>
<tr><td>Name</td><td>Program name</td><td></td><td>Any change</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>Any changes or violations will be reported. There is 1 CO60 record for each I/O Appendage installed on the system.

Current I/O Appendages were verified and stored as the baseline. Additions, deletions, changes and deviations from baseline are automatically reported as discrepancies.</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.

An I/O appendage is a program that provides additional control over system I/O operations. I/O appendages can examine the status of I/O operations and determine actions to be taken under specified conditions. An appendage may receive control in various ways. Appendages receive control in the Supervisor State from the system EXCP processor. These are powerful and must be controlled to avoid compromising system integrity. Appendages can circumvent or disable ACP files, audit trails or access to data. Appendages must be members of the SYS1.LPALIB or SYS1.SVCLIB data sets and must be defined in the IEAAPPxx member of the SYS1.PARMLIB to be available to problem state (unauthorized) programs. A problem state program is one that runs in a protection key greater than 7 and has not been marked as authorized by the Authorized Program Facility.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Technical Services is notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
</table>

Evidence of Review:	AuditStar has an audit trail that keeps track of reviewer, action and dates. Note: This report will be produced **only** when there is a change.

7.7 Shared DASD Across Plexes

<table>
<tr><td>Report Name:</td><td>Shared DASD Across Plexes</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Box_Serial</td><td>Internal serial number(CDA)</td><td>IBM-45-000000000000-0123</td><td></td></tr>
<tr><td>Complex</td><td>Site name</td><td>NEWYORK</td><td></td></tr>
<tr><td>System</td><td>SMF ID</td><td>MVS3</td><td></td></tr>
<tr><td>Shared</td><td>Shared ?</td><td>Yes, No</td><td></td></tr>
<tr><td>Volume_Serial</td><td>Volume Serial</td><td>SMS123</td><td></td></tr>
<tr><td>Device</td><td>Device address</td><td>8F0A</td><td></td></tr>
<tr><td>Unit</td><td>Unit type</td><td>3390</td><td></td></tr>
<tr><td>Mounted</td><td>Mounted ?</td><td>Yes, No</td><td></td></tr>
<tr><td>SMS_managed</td><td>SMS managed ?</td><td>Yes, No</td><td></td></tr>
<tr><td>Warning Id</td><td>Warning number</td><td>1, 2, 3</td><td>2,3</td></tr>
<tr><td>Warning Text</td><td>Warning text</td><td>‘Shared across multiple RACF databases’
‘Inconsistent SHR within complex‘
‘Shared but not configured as SHR‘</td><td></td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>There is 1 CG10 record for every identified DASD volume warning. Any changes or violations will be reported
These are reported as Warnings. The following Warning Text messages indicate possible problems:

‘Inconsistent SHR within complex‘
‘Shared but not configured as SHR‘</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Technical Services is notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
</table>

Report Retention:	6 months
Evidence of Review:	AuditStar has an audit trail that keeps track of reviewer, action and dates. Note: This report will be produced **only** if there is a change.

7.8 SMF Subsystem Parameters

<table>
<tr><td>Report Name:</td><td>SMF Subsystem Parameters
List of all Exit modules defined to the system</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Subsysname</td><td>Subsystem</td><td>SYS, STC, TSO, or a 4 char subsystem id</td><td>Any change</td></tr>
<tr><td>Exitname</td><td>Name of exit program</td><td></td><td>Any change</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>Any changes or violations will be reported.
There is 1 CO41 record for each active exit for each SMF subsystem .
Current SMF Parameters were verified and stored as the standards. Additions, deletions, changes and deviations from standards are automatically reported as discrepancies.</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Technical Services is notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
<tr><td>Evidence of Review:</td><td>AuditStar has an audit trail that keeps track of reviewer, action and dates.
Note: This report will be produced only when there is a change.</td></tr>
</table>

7.9 SAF Router Tables

<table>
<tr><td>Report Name:</td><td>R70: SAF Router Tables</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Class</td><td>Class passed to RACROUTE call</td><td></td><td>Any change</td></tr>
<tr><td>Subsystem</td><td>Subsystem passed to RACROUTE call</td><td></td><td>Any change</td></tr>
<tr><td>Requestor</td><td>Requestor passed to RACROUTE call</td><td></td><td>Any change</td></tr>
<tr><td>Action</td><td>Action to be taken</td><td>RACF, NONE</td><td>Any change</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>Any changes or violations will be reported. There is 1 CR70 record for each class in the Router Table
Current settings were verified and stored as the baseline. Additions, deletions, changes and deviations from baseline are automatically reported as discrepancies.</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Security Analystwill investigate and perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
<tr><td>Evidence of Review:</td><td>AuditStar has an audit trail that keeps track of reviewer, action and dates.
Note: This report will be produced only when there is a change.</td></tr>
</table>

7.10 Started Task Table

<table>
<tr><td>Report Name:</td><td>RC0: Started Task Table</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Procname</td><td>Procedure name (STC name)</td><td></td><td></td></tr>
<tr><td>Userid</td><td>Userid from table</td><td></td><td></td></tr>
<tr><td>Group</td><td>Group from table</td><td></td><td></td></tr>
<tr><td>Attribute</td><td>Privileged or Trusted ?</td><td>Privileged, Trusted</td><td></td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>Any changes or violations will be reported. There is 1 CRC0 record for each entry in ICHRIN03. This table should always be empty.
Current settings were verified and stored as the baseline. Any addition to the table is automatically reported as a discrepancy.</td></tr>
<tr><td>Run Cycle:</td><td>Daily – Business Days</td></tr>
<tr><td>Resource:</td><td>Automated</td></tr>
<tr><td>Reviewer:</td><td>Security Analyst</td></tr>
<tr><td>Media:</td><td>Online</td></tr>
<tr><td>Baseline:</td><td>Yes. Standards are stored and data is automatically compared against the standard.</td></tr>
<tr><td>Review Criteria:</td><td>Report flags any changes listed in the Monitor Changes column.
This table should always be empty.</td></tr>
<tr><td>Actions:</td><td>When problems are found, Security Analystwill investigate and perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.</td></tr>
<tr><td>Action Taker:</td><td>Security Analyst</td></tr>
<tr><td>Report Retention:</td><td>6 months</td></tr>
<tr><td>Evidence of Review:</td><td>AuditStar has an audit trail that keeps track of reviewer, action and dates.
Note: This report will be produced only when there is a change.</td></tr>
</table>

7.11 Resource Profile

<table>
<tr><td>Report Name:</td><td>P21: Resource Access</td></tr>
<tr><td>Environment:</td><td>IBM HOST</td></tr>
<tr><td>Application:</td><td>Auditstar</td></tr>
<tr><td>Report Description:</td><td>
<table>
<tr><th>Field name</th><th>Information in field</th><th>Possible values</th><th>Monitored controls</th></tr>
<tr><td>Class</td><td>Resource class</td><td></td><td>Any change</td></tr>
<tr><td>Profilekey</td><td>Profile key</td><td></td><td>Any change</td></tr>
<tr><td>Profile type</td><td>Discrete or generic</td><td></td><td>Any change</td></tr>
<tr><td>AccessID</td><td>AccessID (userid or group)</td><td></td><td>Any change</td></tr>
<tr><td>Accesslevel</td><td>Accesslevel</td><td></td><td>Any change</td></tr>
<tr><td>Condtype</td><td>Type of conditional access</td><td>PROGRAM, TERMINAL, APPCPORT etc</td><td>Any change</td></tr>
<tr><td>Condname</td><td>Conditional resource name</td><td></td><td>Any change</td></tr>
</table>
</td></tr>
<tr><td>Security Controls:</td><td>Any changes or violations will be reported.

There should be 1 CP21 record for each profile in the following general resource classes:

APPCLU, APPCPORT, APPCSERV, APPCTP, APPCSI, APPL, CONSOLE, DEVICES, FIELD, GSDSF, GTERMINL, ILMADMIN, JESINPUT, JESJOBS, JESSPOOL, LOGSTRM, NETCMDS, NETSPAN, NODES, OPERCMDS, PROGRAM, PROPCNTL, PTKTDATA, RRSFDATA, SDSF, SECDATA, SURROGAT, TERMINAL, TSOAUTH, TSOPROC, UNIXPRIV, VTAMAPPL, WRITER, %CICSCMD.

There is 1 CP21 record for any profile matching the following masks in the FACILITY class:
BPX*.**
CSV*.**
ICH*.**
IEA*.**
IEC.TAPERING
IGG*.**
IHJ*.**
IHV*.**
IRR*.**
IXF*.**
VRA$.**
DITTO.**</td></tr>
</table>

	FILEAID.** **MVSADMIN.**** **STGADMIN.**** There is 1 CP21 record for any profile matching the following masks in **any** general resource class: **$CNF*.**** **$CNG*.**** **$C2R*.**** **$C4R*.**** There is 1 CP21 record for any profile containing the following strings in any **%CICSTRN** class: **CECI** **CEDA** **CEDB** **CEDF** **CEMT** **CETR** **CWTO** Additions, deletions, changes and deviations from standards are automatically reported as discrepancies.
Run Cycle:	Daily – Business Days
Resource:	Automated
Reviewer:	Security Analyst
Media:	Online
Baseline:	Yes. Standards are stored and data is automatically compared against the standard.
Review Criteria:	Report flags any changes listed in the Monitor Changes column.
Actions:	When problems are found, Technical Services is notified so they can perform further analysis. When corrective action is taken it will be reported automatically by AuditStar.
Action Taker:	Security Analyst
Report Retention:	6 months
Evidence of Review:	AuditStar has an audit trail that keeps track of reviewer, action and dates.

8. Additional System Reports

The following table lists all of the reports that are available in AuditStar.

Report No.	Report Name	What to look for	Examples of concerns
O10	IPL volume and device unit address		
O30	SMF parameters	Global settings for SMF recording	Inactivating SMF
O40	SMF subsystem exit detail	The subsystem and exit name for SMF exits on the system	New exits should be audited to assure system integrity
O41	SMF subsystem exit activity	SMF exits interval recording time, and suppressed record types. Also indicates if detailed activity recording is on or off.	Any changes in the recording of exits should be investigated.
O42	SMF subsystem recording inactivity	There is no logging of activity for suppressed SMF records	Any new suppressed record types must be investigated because audit trails (RACF 80 Dataset I/O) for these events will not be available
O50	Supervisor Calls (SVCs)	New, altered or removed SVCs	Rogue SVCs can provide an entry point to bypass security and resource protection thereby gaining unauthorized access to sensitive or system data.
O51	Supervisor Calls (SVCs Details)	New, altered or removed SVCs with more detail than O51. This record is never processed for discrepancies but is available to provide edification	Rogue SVCs can provide an entry point to bypass security and resource protection thereby gaining unauthorized access to sensitive or system data.
O60	I/O Appendages	New, altered or removed appendages	Appendages that have been added or deleted
O61	I/O Appendages (Details)	New, altered or removed appendages	Appendages that have been added or deleted
O71	Program Calls		
O80	MVS Subsystem Appendages	New, altered or removed appendages	Appendages that have been added or deleted
O90	Modules with Scan Hits	Modules that have suspicious instructions	Programs that appear to be setting authorization/authority bits: FakeSpecial (flipping bit in ACEE); FakeOperations (ACEE); FakePriv (ACEE).
O91	Monitored Load Modules	Changes in modules that have been specifically identified to be watched	Unexpected changes
O92	Monitored Text Members	Changes in text that have been specifically identified to be watched	Unexpected changes

Report No.	Report Name	What to look for	Examples of concerns
P51	Sensitive Datasets - dsnames	See list of automatically detected system datasets	Unexpected changes
P60	RACF Segment Usage	Indicates number of profiles in the RACF database	For Information Only
P61	RACF Database Size	Indicates size of RACF database in terms of Bytes	For Information Only
R10	System software releases and status (RACF only)	RACF, DFP, HSM, JES, MVS, RMF, SMS, TSO, VTAM	An unexpected RACF upgrade / regression
R15	CONSOLES logon required	System consoles - security settings	Unexpected changes
R21	SETROPTS – part a	System wide RACF settings	Unexpected changes
R22	SETROPTS – part b	System wide RACF settings	
R23	SETROPTS – part c	System wide RACF settings	
R30	RACF Database Name Table	Names of your RACF datasets	Changes to table
R32	RACF Database Range Table	If you have multiple RACF datasets, this table specifying which profiles go on which dataset	Changes to table
R40	RACF Authorized Caller Table	Programs that can run APF authorized within TSO	New programs
R51	RACF Class Descriptor Table – details a	All RACF classes and their attributes	New classes; Deleted classes; Activation/inactivation of a class; modification to characteristics of a class
R52	RACF Class Descriptor Table – details b	All RACF classes and their attributes	New, deleted, ensure classes are directed to RACF
R60	RACF Global access table (GLOBAL class)	GLOBAL class entries have no SMF auditing	Unexpected changes
R70	SAF Router Table	MVS SAF table that routes SAF requests	
R80	Modules with PPT attributes	APF Modules, their library and access list for programs that are present in the PPT with BYPASS or a system key, or TSO authorizations (AuthCMD, AuthPGM, AuthTSF).	Any modules that can bypass RACF
RB2	System exits	See table of exits	RACF exits; SMF exits; Exits can modify expected security behavior; can modify SMF data
RC0	RACF Started Task Table (ICHRIN03)	Contents of table ICHRIN03	Started tasks with TRUSTED or PRIVILEGED
P10	RACF dataset profiles to be monitored	Monitor dataset profiles that do not comply with standard / policy; Monitor dataset profiles of identified "sensitive" datasets	Installation specific violations of standards for profiles.
P11	RACF dataset profiles to be monitored – Access lists	Access lists of above profiles.	

Report No.	Report Name	What to look for	Examples of concerns
P20	RACF general resource profiles to be monitored	Monitor protection of system wide general resources, e.g. MVS operator commands; JES commands; CICS / IMS transactions…	
P21	RACF general resource profiles to be monitored – Access lists		
P22	RACF general resource profiles to be monitored – Members		
P30	RACF dataset profiles for Sensitive Datasets	Dataset profiles for datasets that are critical to the integrity of the operating system	Unexpected changes
P31	RACF dataset profiles for Sensitive Datasets – Access lists		UPDATE access (or higher)
P40	RACF STDATA segments for STARTED class	All STDATA segments in STARTED class	Started tasks with TRUSTED or PRIVILEGED
U10	RACF Userids with system attributes/privileges	Special attributes: Userids that have the system-SPECIAL attribute can issue any RACF command and can change any RACF profile except for some auditing-related operands; OPERATIONS is like a "back door" to dataset access; AUDITOR allows you to look at any RACF profile, and change global auditing settings	These are highly privileged users somewhat equivalent to root in Unix. Verify any new or removed users.
U11	RACF Userids that are audited	Userids that have the UAUDIT attribute set. Actions by these userids always create an audit trail.	Verify any new users or users that have been removed.

Report No.	Report Name	What to look for	Examples of concerns
U12	RACF Userids that are protected	These userids are ones which cannot be used to logon (or start a batch job) with a password. For example, you might use these for started tasks, so that the userids can only be used for started tasks. (This would prevent someone from guessing (or remembering) the password of a started task's userid and using it on a batch job to hack your system.) Protected userids cannot be revoked by entering a bunch of bad passwords.	Protected userids make sense for started tasks (including RACF itself), for OMVS and TCP/IP daemons, for CICS default userids, and for CICS pre-defined terminal userids. Verify any new or removed protected userids.
U13	RACF Userids that are restricted.	A Restricted userid is granted access to a dataset or resource if and only if its userid or group is explicitly permitted to the dataset or resource rule. This means that the RACHECK and FRACHECK basic RACF functions will NOT grant such userids access based on: UACC, ID(*) or GLOBAL rules The Restricted attribute has no effect for UNIX files in the HFS or for datasets and resources marked WARNING.	Restricted userids are a solution for controlling access by guest users such as those entering via a web browser. Verify any new or removed restricted userids.
U21	RACF Userids with Class Authorizations	Users who have class authorizations (CLAUTH). The CLAUTH (class authority) attribute allows a userid to define RACF profiles in specified RACF classes.	Verify any new users
U31	RACF Groups to be monitored	Groups that have access to sensitive data and/or commands	Verify any new members in these groups are OK
U40	RACF Userids with non-conforming password interval	Users with password interval other than 30	Verify any user who has NOINTERVAL
U50	RACF ‘Critical’ userids that are revoked	"Hot ids", CA7 ids, AutoOps ids etc	Could cause outages
U60	RACF Userids that have never been used, Created > nn days ago	Userid probably not needed	Cleanup / housekeeping

Report No.	Report Name	What to look for	Examples of concerns
U70	RACF Userids that are inactive, Last Use > mm days ago	"Stale" userids, probably not needed any more	Cleanup / housekeeping
U80	RACF Userids with Group attributes/privileges	All users with either GROUP SPECIAL, OPERATIONS, AUDITOR. Userids that have the group-SPECIAL attribute can issue any RACF command and can change any RACF profile within the scope of the applicable group except for some auditing-related operands; Userids with OPERATIONS can access any group resource.	Verify any new users - allows administrative capabilities within RACF
U90	Sensitive Unix UIDs	Sensitive UIDs that should or should not exist. (UID of 0 is superuser in OMVS. Users can also get via access to BPX.SUPERUSER)	Verify that sensitive UIDs exist
U91	Users with Sensitive Unix UIDs	UID of 0 is superuser in OMVS (Can also get via access to BPX.SUPERUSER)	Verify that Users with sensitive UIDs are restricted to those authorized
U95	Sensitive Unix GIDs	Some GIDs may be restricted	Verify that restricted GIDs exist are not used by unauthorized groups
U96	Groups with Sensitive Unix GIDs	Groups with sensitive GIDs may be restricted	Verify that Groups with sensitive GIDs are restricted to those authorized
U97	Users in Groups with Sensitive Unix GIDs	Users in Groups with sensitive GIDs may be restricted	Verify that Users in Groups with sensitive GIDs are restricted to those authorized