VANGUARD
INTEGRITY PROFESSIONALS, INC.
enterprise security software

Using Vanguard Configuration Manager for Continuous Monitoring of NIST Security Controls on the IBM z/OS Operating System Environment.

In General

General Information:

Session will be using the current version of the DISA STIG checklist. The DISA Checklist is generally ahead of the NIST checklists posted to the NCP.

Disclaimers:

Some of the checks in the checklist may not be applicable to you.

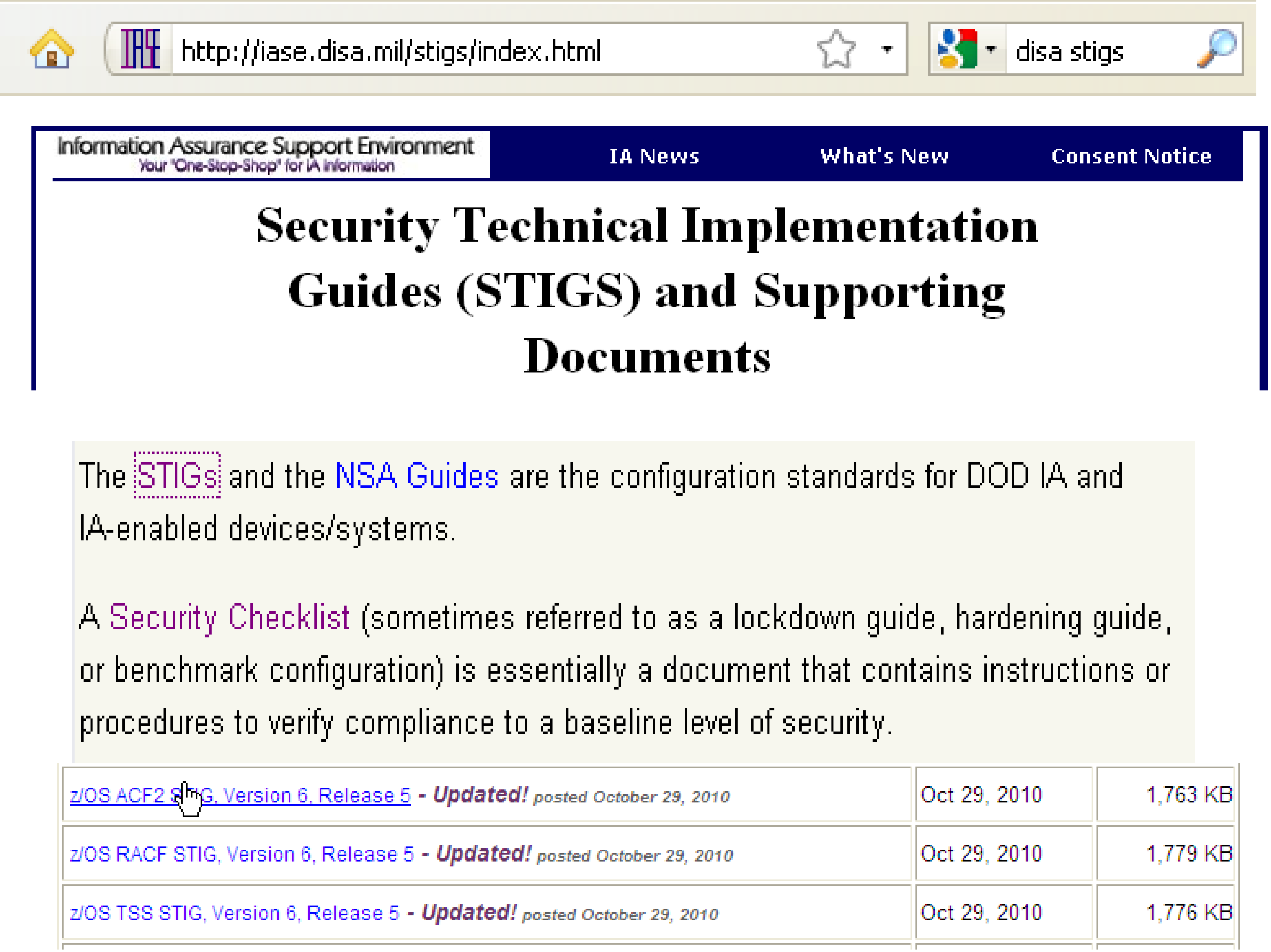
You may not be able to implement some of the checks/requirements in your environment.

Some checks are open to interpretation. The presenter does not represent DISA and is only presenting his opinion and observations.

What is Vanguard Configuration Manager?

- Vanguard Configuration Manager™ (VCM) is an automated vulnerability assessment solution that assists organizations in passing a Security Readiness Review (SRR) for IBM® OS/390® & z/OS® RACF®.
- Passing a Security Readiness Review (SRR) brings the mainframe system security into compliance to the Security Technical Implementation Guide (STIG) published by the Defense Information Security Agency (DISA) for the Department of Defense (DoD) and National Institute of Standards and Technology (NIST) in the National Checklist Program (NCP).
- These guidelines are considered by some in the industry as “Core Security Requirements” (CSRs).

The DISA STIGs



http://iase.disa.mil/stigs/index.html
disa stigs
Information Assurance Support Environment
Your 'One-Stop-Shop' for IA information
IA News
What's New
Consent Notice

Security Technical Implementation Guides (STIGS) and Supporting Documents

The STIGs and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems.

A Security Checklist (sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration) is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

z/OS ACF2 STIG, Version 6, Release 5 - ***Updated!*** *posted October 29, 2010*	Oct 29, 2010	1,763 KB
z/OS RACF STIG, Version 6, Release 5 - ***Updated!*** *posted October 29, 2010*	Oct 29, 2010	1,779 KB
z/OS TSS STIG, Version 6, Release 5 - ***Updated!*** *posted October 29, 2010*	Oct 29, 2010	1,776 KB

The DISA STIGs

z/OS RACF STIG Checklist
Version 6, Release 9
27 Oct 2011

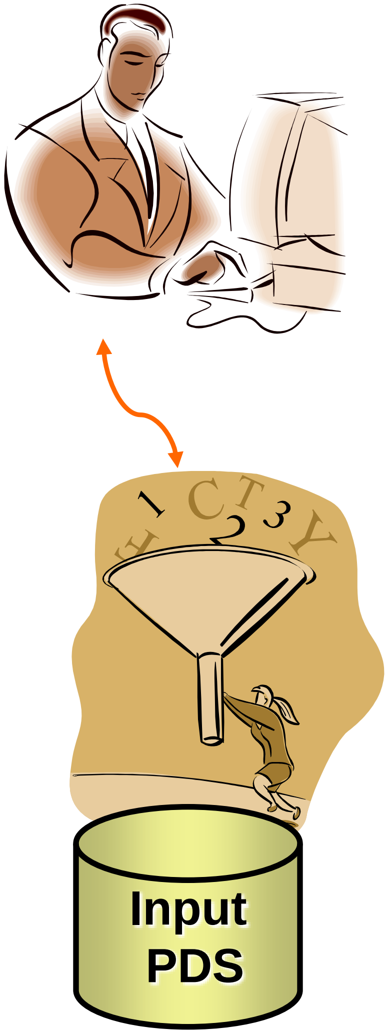
Vanguard Configuration Manager - Features

- Vanguard Configuration Manager includes:
  - an interview process for data collection
  - an automated data analysis process *
  - summary-level and detail-level reporting *

  * Available Online and in Batch

- Vanguard Configuration Manager speeds the data collection process by ensuring that your answers are saved across checks that require the same data.

- Vanguard Configuration Manager saves the answers for each interview question, so you don't have to recollect the information required for subsequent reviews.



Vanguard Configuration Manager Phases

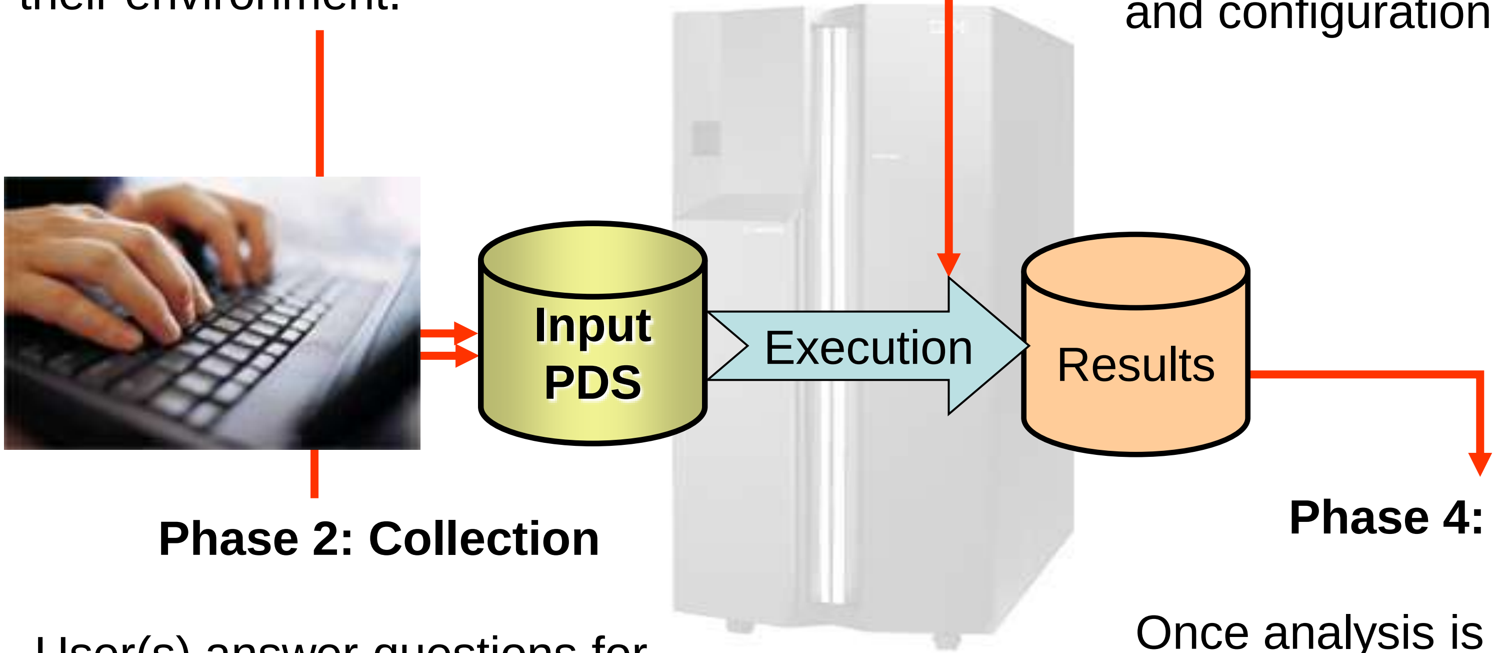
Overview of Phases

Phase 1: Common Configuration

User(s) complete all relevant Common Configuration questions for their environment.

Phase 3: Execution

The Input PDS is used for an analysis of the system settings and configurations.



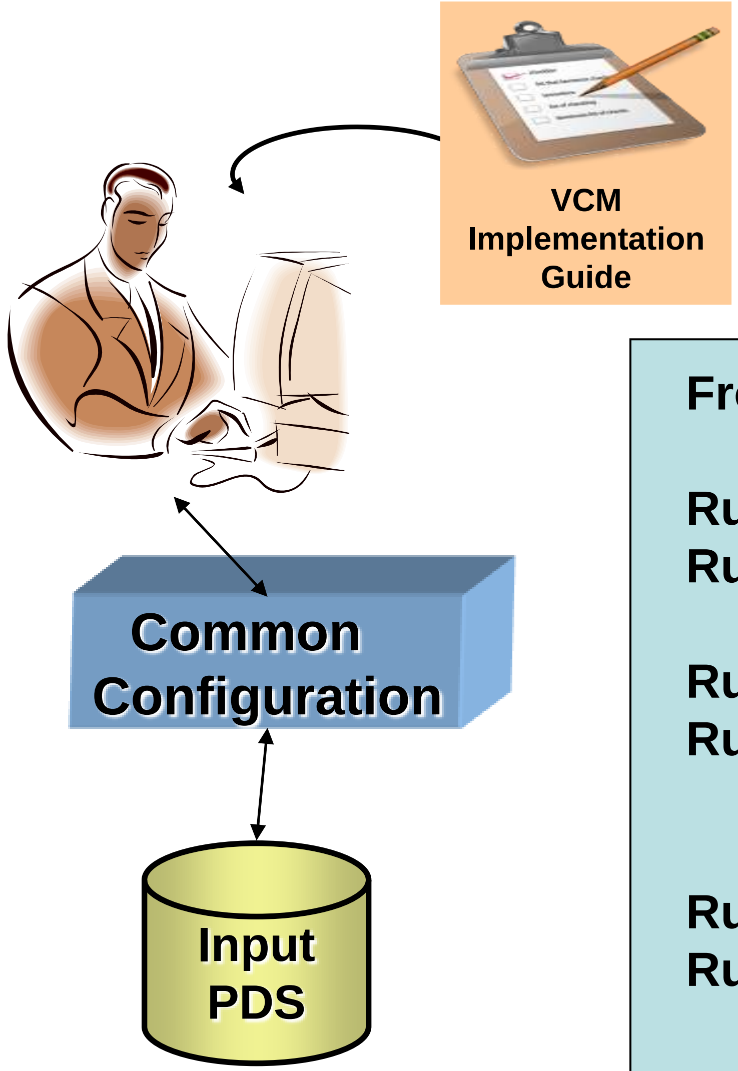
Phase 2: Collection

User(s) answer questions for specific checks which provides information about current system settings and configurations.

Phase 4: Results

Once analysis is complete, the results are displayed as Findings, No Findings or Informational messages.

Common Configuration

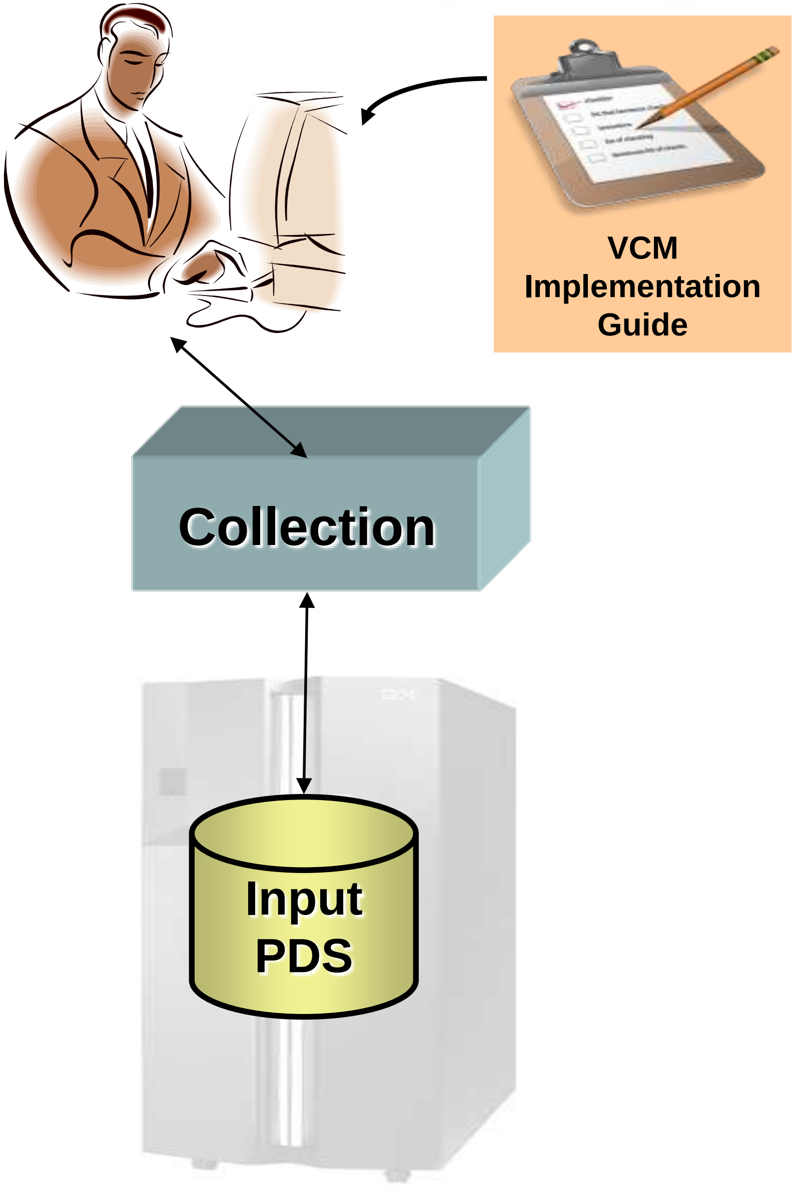


Common Configuration (ACOM) expedites the interview process by providing a central data repository from which the checks can share information.

From the DISA STIGs version 6.8

Rule Version (STIG-ID): ACP00010
Rule Title: SYS1.PARMLIB is not limited to only system programmers.
Rule Version (STIG-ID): ACP00110
Rule Title: Update and allocate access to LINKLIST libraries are not limited to system programmers only.
Rule Version (STIG-ID): ACP00180
Rule Title: Update and allocate access to SMF collection files (i.e., SYS1.MANx) are not limited to system programmers and/or batch jobs that perform SMF dump processing.

Collection



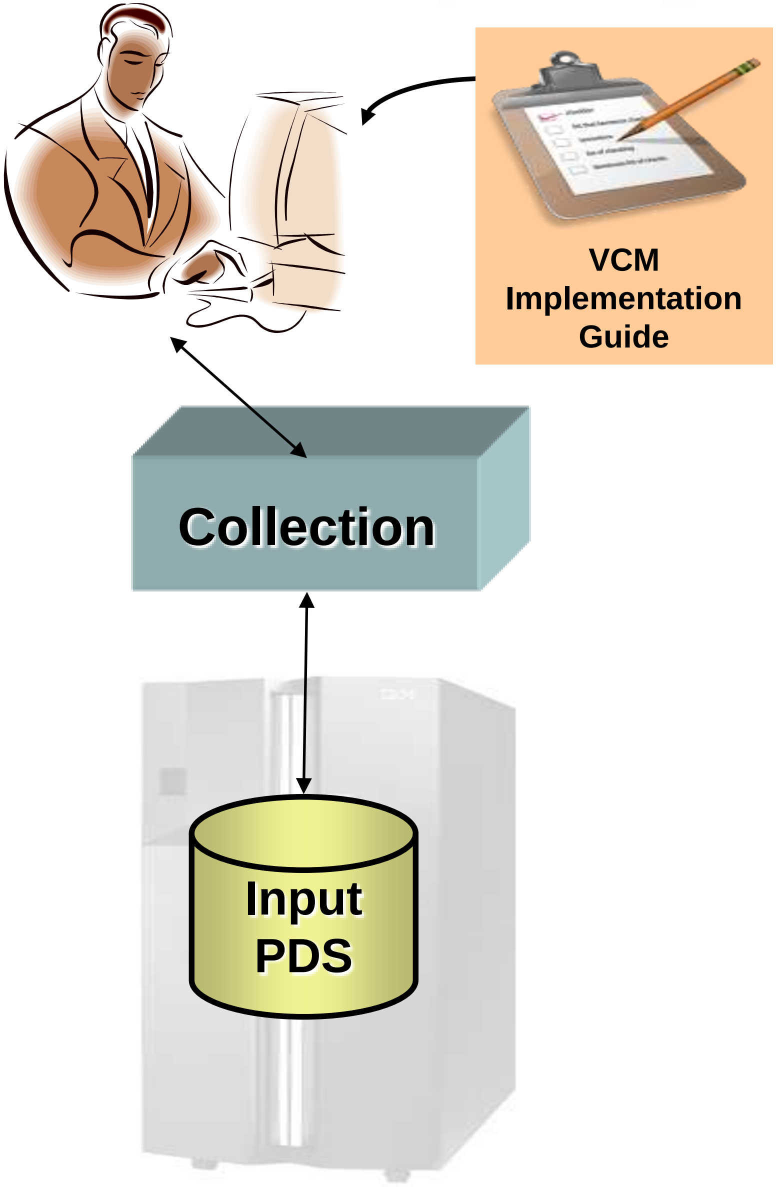
Collection can be done on a Single Check by placing a C next to the check. Multiple checks can be collected by placing a Cxx (where xx is the number to collect) next to the first check.

Some Checks are completely automated and require no Input. These will be indicated by --- (3 dashes) under the Collected Stat Heading.

If the data for a check is derived from a Common Configuration Member, that data will automatically be presented to the user at data collection time.

Input derived from a Common Configuration Member can be modified. The changes are saved in the check being collected and have no affect on the Common Configuration Member. This is referred to as Delta Processing.

Collection



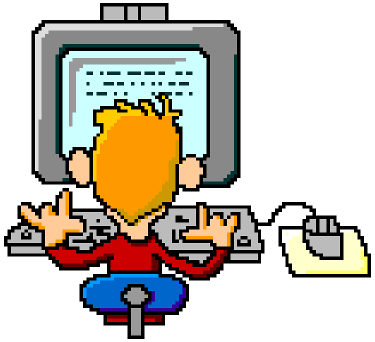
Data required not stored in a Common Configuration Member will cause a panel to prompt for the required input.

Some Data Input is Optional. This will be reflected on the panel by this text: If request is not applicable, leave input field(s) blank.

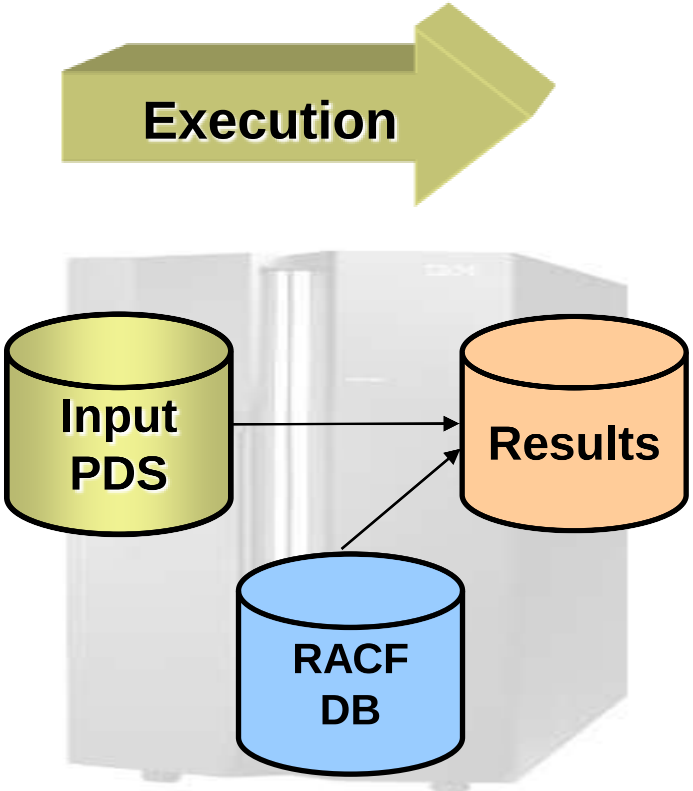
Extensive Online Help is available.

Once data is collected it will indicate who collected the data and when it was collected

Data collection by default is forced again after 30 days. This is controlled by the DAYS_VALID parm in the VCMOPT00 member.



Execution



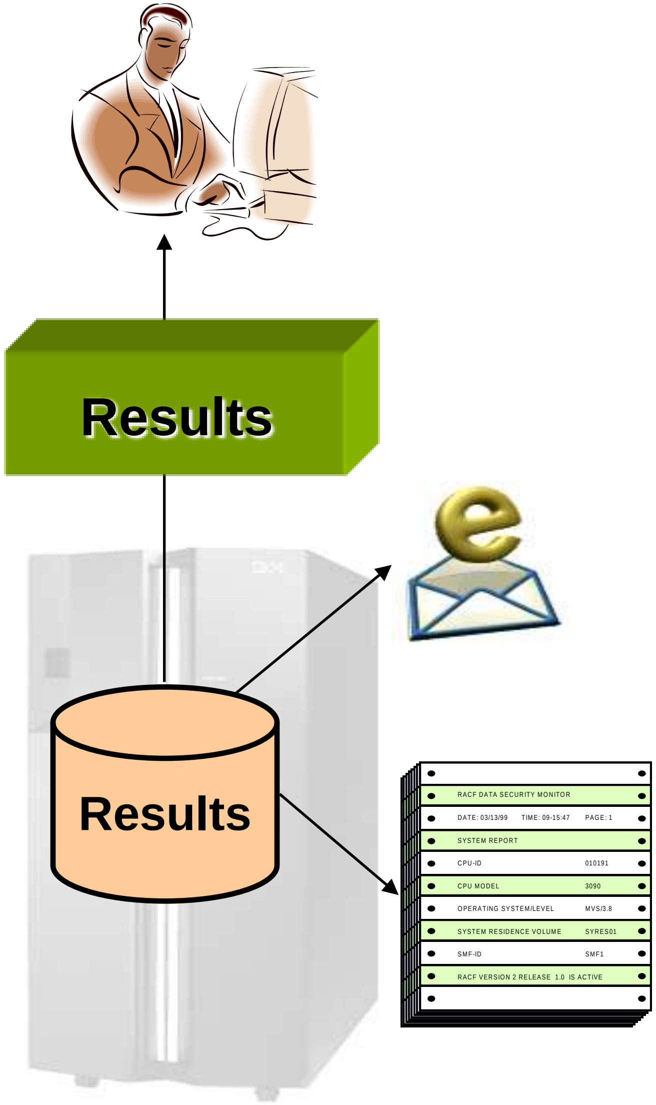
During Execution of the checks, Vanguard Configuration Manager uses the information you provided to perform an analysis, or audit, of the system settings and configurations.

The output of the checks will be placed in the Results Dataset.

Execution can be done on a Single Check Basis by placing an E next to the check. Multiple checks can be executed by placing an Exx (where xx is the number to execute) next to the first check.

Execution of checks can be done online or in batch.

Results



```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

The Results of the Execution are stored in the Output Results Dataset.

Results are issued as Finding, No Finding, Informational or Error Messages.

The Final Execution Result of a particular check is based on the following hierarchy, listed under Execution Results:

1. Error
2. Finding
3. No Finding
4. Not Applicable
5. Never Run

Note: Each Message in the results file will have a message number in the following format:
STIGID - Message Number Message Type

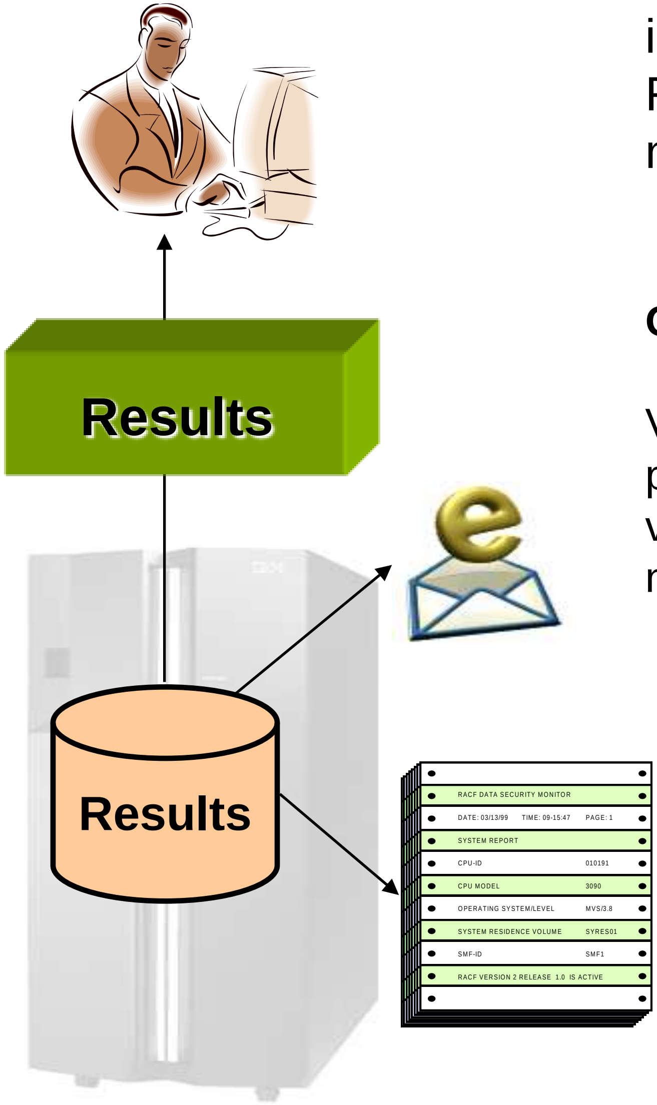
Ex: RACF0480-04N

Results

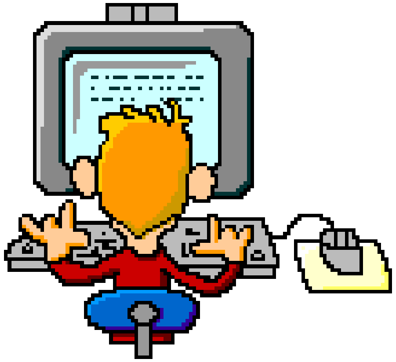
Viewing Results – You can view the results of individual checks in order to review the FINDING, NO FINDING, INFORMATIONAL and ERROR messages.

ONLINE:

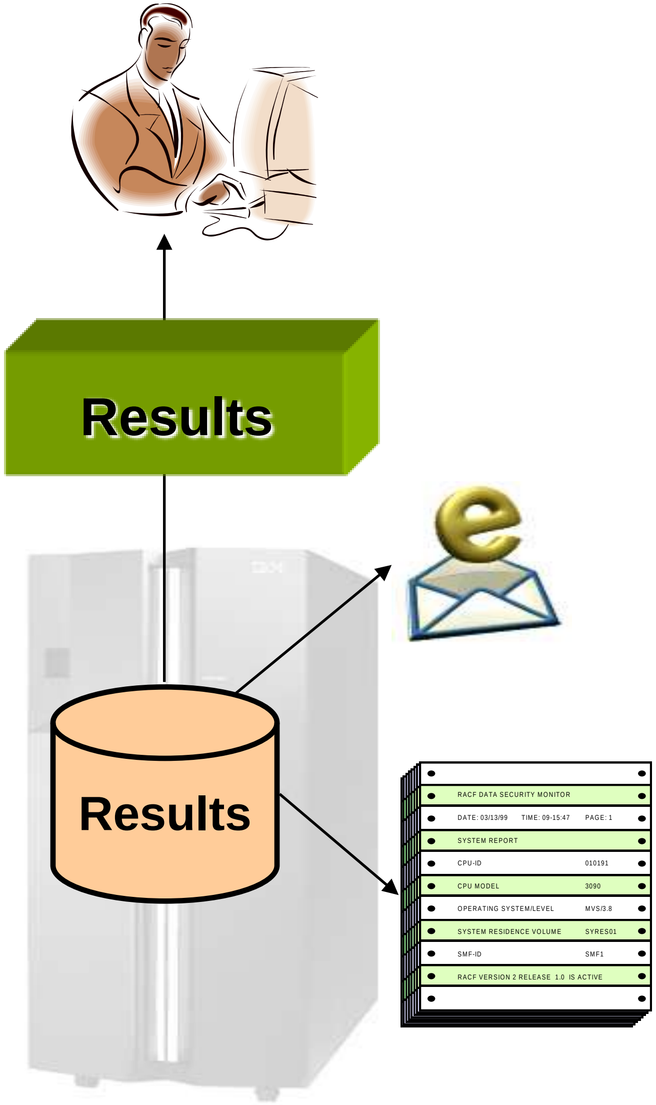
Viewing Results can be done on a Single Check Basis by placing a V next to the check. Multiple checks can be viewed by placing a Vxx (where xx is the number to view) next to the first check.



```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```



Results



```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

Summary Reports – allow the ability to generate *predefined* summary reports on all checks or a per category basis.

ONLINE:

A Full Summary Report will be generated by choosing Summary Report from the Report Menu on the Toolbar.

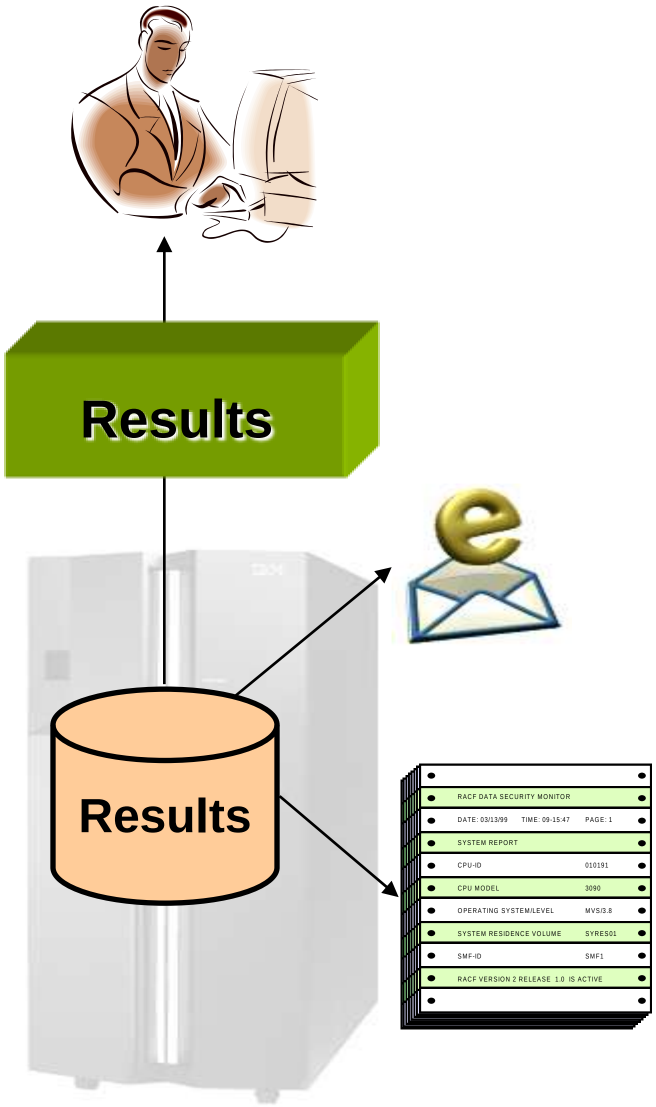
A Per Category Report will be generated by placing an R next to the Category from the Main Menu.

BATCH:

A Full Summary Report will be generated by including the SUMMARY Control Statement under the DD SCNINPUT.

A Per Category Report will be generated by including the CATSUMMARY Control Statement under the DD SCNINPUT followed by the name or names of the Categories.

Results



```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

Detailed Reports – allow the ability to generate a *predefined* detail reports which display among other things, all the messages related to the particular check.

ONLINE:

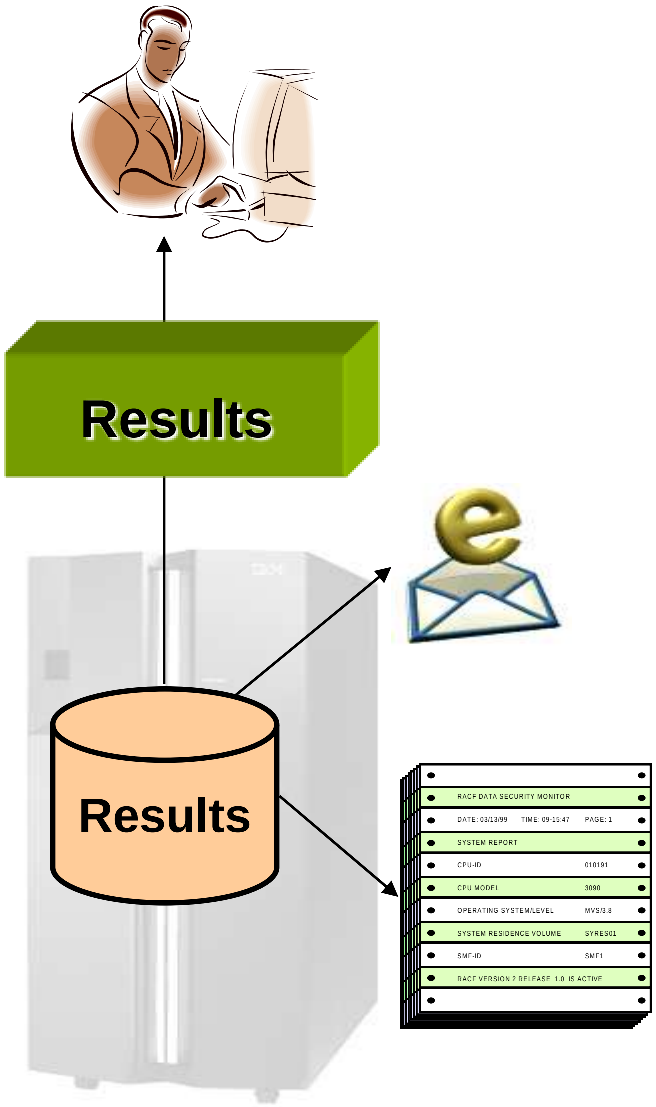
A Detailed Report of a Particular Check can be generated by placing an R next to the Check. Note: In this mode the report will be placed into a browse dataset that you can search.

BATCH:

A Detailed Report will be generated by including the REPORT Control Statement followed by the Name or Names of the Checks under the DD SCNINPUT.

Note: The generated JCL will include all checks based on the filter set in VCM.

Results



```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                               010191
CPU MODEL                            3090
OPERATING SYSTEM/LEVEL               MVS/3.8
SYSTEM RESIDENCE VOLUME              SYRES01
SMF-ID                               SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

Compare Results– allows for a user to compare their current results with a previous results and get a report on the Delta's Only.

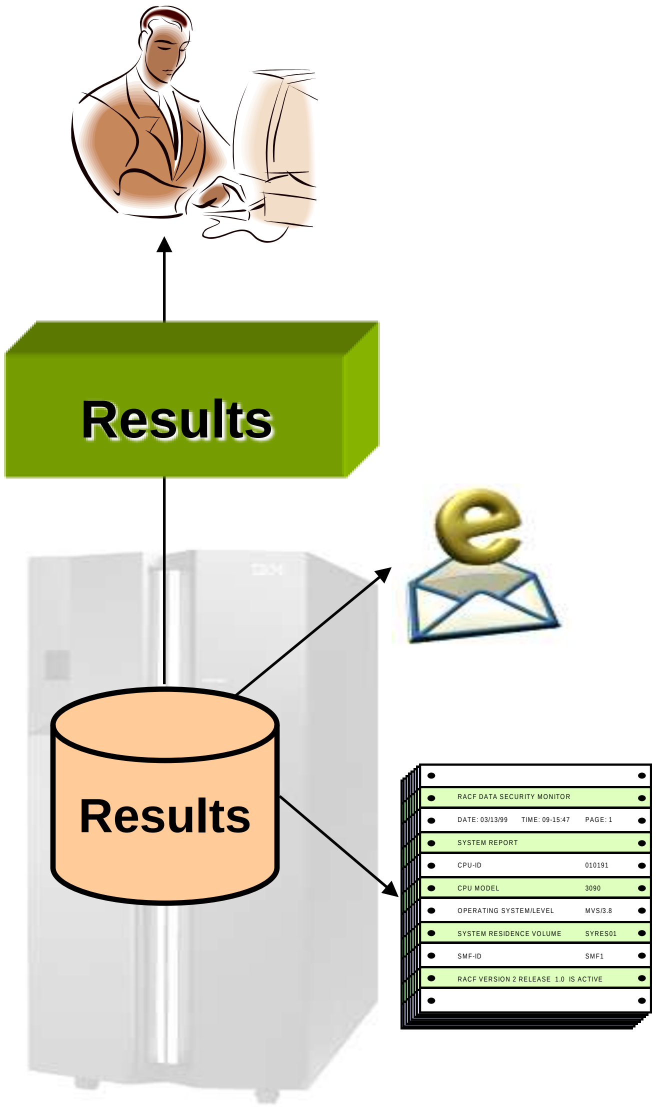
ONLINE:

Select the Check that you want the comparison run, and then chose the two results sets to compare. NOTE: More than one result set must exist for the comparison feature to be run.

BATCH:

A Detailed Compare Report will be generated by including the COMPRE(x,y) Control Statement followed by the Name or Names of the Checks under the DD SCNINPUT.

Results



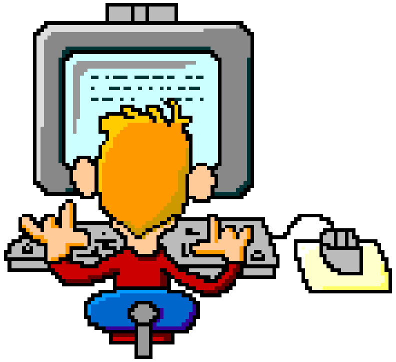
```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

E-mailing and Printing Reports

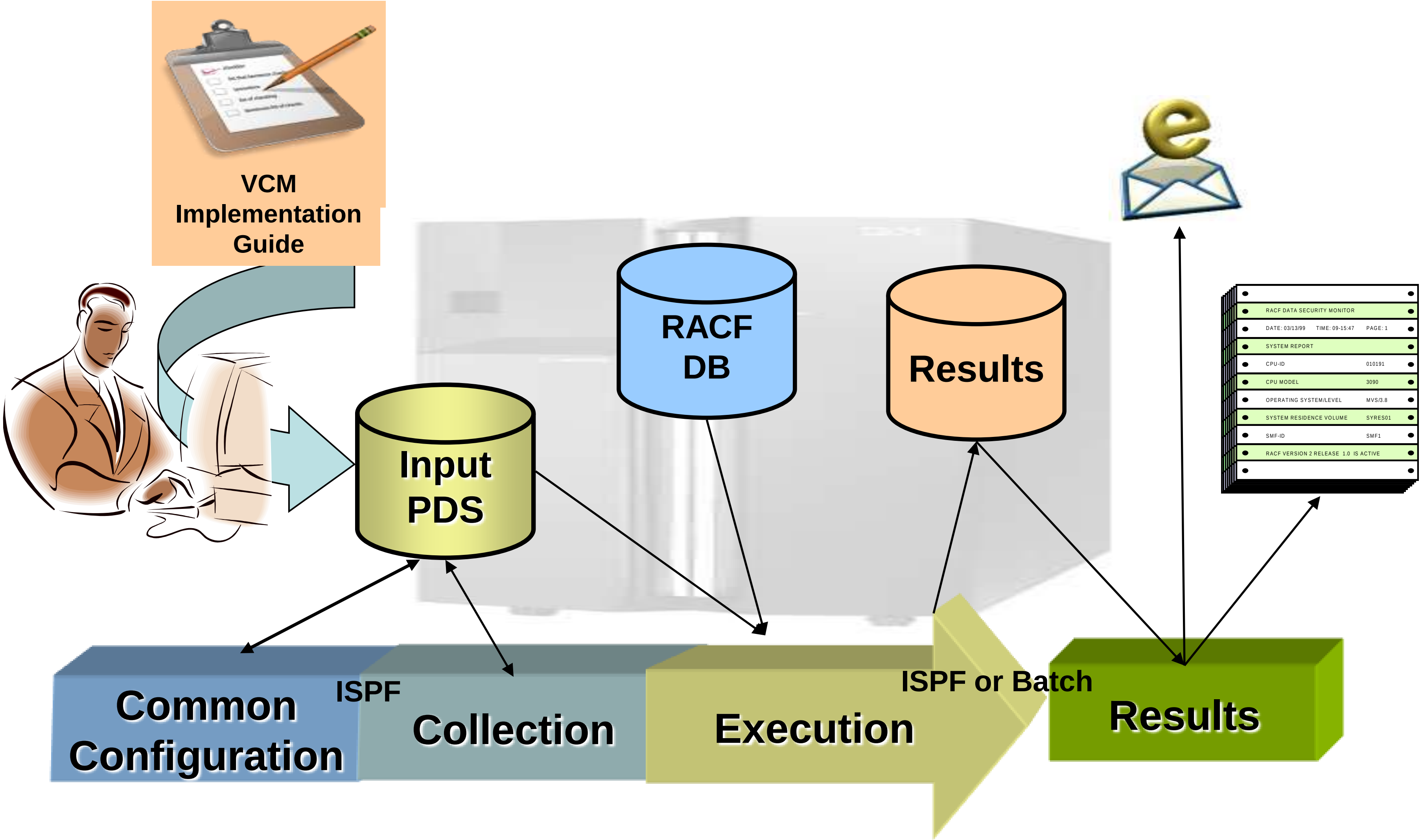
Online:

From within the Report screen you can send the report as an e-mail using the EMAIL primary command.

From within the Report screen you can print the report using the PRNT primary command.



Review



VCM Implementation Guide

Input PDS

RACF DB

Results

```
RACF DATA SECURITY MONITOR
DATE: 03/13/99      TIME: 09-15:47      PAGE: 1
SYSTEM REPORT
CPU-ID                                  010191
CPU MODEL                               3090
OPERATING SYSTEM/LEVEL                  MVS/3.8
SYSTEM RESIDENCE VOLUME                 SYRES01
SMF-ID                                  SMF1
RACF VERSION 2 RELEASE  1.0  IS ACTIVE
```

Common Configuration

ISPF

Collection

Execution

ISPF or Batch

Results

Demo Time

DEMO TIME

In this DEMO we will run a couple checks and change the environment to see the impact on the checks.

Checks:

AAMV0050

ACP00282

ZUSS0047

Demo Time

Rule Version (STIG-ID): AAMV0050
Rule Title: Duplicated sensitive utilities and/or programs exist in APF libraries.

Vulnerability Discussion: Modules designated as sensitive utilities have the ability to significantly modify the operating system environment. Duplication of these modules causes an exposure by making it extremely difficult to track modifications to them. This could allow for the execution of invalid or trojan horse versions of these utilities.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCSL-1

Check Content:

a) If duplicate APF modules exist, compare the duplicates to the modules specified below:

The following list contains Sensitive Utilities that will be checked.

AHLGTF AMASPZAP AMAZAP AMDIOCP AMZIOCP
BLSROPTR CSQJU003 CSQJU004 CSQUCVX CSQUTIL
CSQ1LOGP DEBE DITTO FDRZAPOP GIMSMP
HHLGTF ICKDSF ICPIOCP IDCSC01 IEHINITT
IFASMFDP IGWSPZAP IHLGTF IMASPZAP IND$FILE
IOPIOCP IXPIOCP IYPIOCP IZPIOCP WHOIS
L052INIT TMSCOPY TMSFORMT TMSLBLPR TMSMULV
TMSREMOV TMSTPNIT TMSUDSNB

b) If none of the sensitive utilities are duplicated, there is NO FINDING.

c) If any of the sensitive utilities is duplicated, this is a FINDING.

Demo Time

Rule Version (STIG-ID): ACP00282
Rule Title: z/OS system commands are improperly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control access to z/OS system commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:
a) The MVS.** resource is defined to the OPERCMDS class with a default access of NONE and all (i.e., failures and successes) access logged.

b) Access to z/OS system commands defined in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

c) All access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum.

d) If either (a),,(b), or (c) above is untrue for any z/OS system command resource, this is a FINDING.

e) If (a), (b), and (c) above are true, there is NO FINDING.

Demo Time

Rule Version (STIG-ID): ZUSS0047
Rule Title: z/OS UNIX user accounts are not properly defined.

Vulnerability Discussion: User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Responsibility: Information Assurance Officer

IAControls: DCCS-1, DCCS-2

Check Content:

NOTE: This check only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

a) If each user account is defined as follows, there is NO FINDING:

1) A unique UID number (except for UID(0) users)
2) A unique HOME directory (except for UID(0) and other system task accounts)
3) Shell program specified as “/bin/sh”, “/bin/tcsh”, “/bin/echo”, or “/bin/false”

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

b) If any user account is not defined as specified in (b) above, this is a FINDING.

Questions?