

NIST Standards and a VCM Implementation

Mike Wenger
Wisconsin Physicians Service
Madison, WI

15 Aug, 2013
Session Number 14031

The NIST STANDARDS by FAMILY

The Nist Standard by Family and Government Specification

About WPS – Challenges and Opportunities

VCM – Phases and usage

WPS – Experience

Wrapup

The NIST STANDARDS by FAMILY

Access Control

**FIPS 200 and 201
SP 800-53**

Audit & Accountability

**FIPS 200
SP 800-137**

Awareness & Training

**FIPS 200
SP 800-53
SP 800-50**

Certification, Accreditation & Security Assessments

**FIPS 200
SP 800-126
SP 800-117**

Configuration Management

**FIPS 200
SP 800-126
SP 800-53**

Contingency Planning

FIPS 200

The NIST STANDARDS by FAMILY

Identification & Authentication

FIPS 201
FIPS 200
SP 800-53

Incident Response

FIPS 200
SP 800-126

Maintenance

FIPS 200
SP 800-126
SP 800-53

Media Protection

FIPS 200
SP 800-124
SP 800-53

Personnel Security

FIPS 200
SP 800-53

The NIST STANDARDS by FAMILY

Physical & Environmental Protection

FIPS 200
SP 800-123

Planning

FIPS 201
FIPS 200
SP 800-153

Risk Assessment

FIPS 199
FIPS 200
SP 800-53
SP 800-137

System & Communications Protection

FIPS 197
FIPS 198
FIPS 200
FIPS 201

The NIST STANDARDS by FAMILY

Physical & Environmental Protection

FIPS 200
SP 800-123

Planning

FIPS 201
FIPS 200
SP 800-153

Risk Assessment

FIPS 199
FIPS 200
SP 800-53
SP 800-137

System & Communications Protection

FIPS 200
FIPS 201

The NIST STANDARDS by FAMILY

System & Information Integrity

FIPS 200

FIPS 140

SP 800-53

System & Services Acquisition

FIPS 200

SP 800-147

NIST 800-126

NIST 800-126 is the Technical Specifications for the Security Content Automation Protocol

NVD and NCP are the centralized repository for all vulnerabilities and checklists

Wisconsin Physicians Service

- WPS
 - Who We Are
 - Our Challenge
 - Our Opportunity
- What is VCM?
- Our Experience

WPS

- Major Health Insurance Provider in Mid-West
- Over 5 million Claims Processed Per Month
 - WPS Health Insurance
 - TRICARE
 - Medicare

Our Challenge

- Multiple Government Agency Security Compliance
- Audits Overwhelming
 - More than 18 Different Audits Annually
 - Most Comprehensive Used to Respond to All
 - Government Most Complex/Consuming
 - TRICARE - DIACAP Requirements (ATO)
 - Medicare – CMSR, Section 912, etc.

Our Challenge

- DIACAP Authority to Operate (ATO) Most Comprehensive
 - TRICARE Management Authority (TMA)
 - Annual Multiple Month Process
 - Significant Manual Effort
 - Significant Impact on Normal Operations

Our Challenge

- TMA Monthly Site CD
 - CA-Examine Based Scripts
 - Based on DoD/DISA STIGs
 - Department of Defense (DoD)
 - Defense Information System Agency (DISA)
 - Security Technical Implementation Guide (STIG)
 - Results Used for Other Audits, But Clumsy

Our Opportunity

- TMA Shifted Annual Certification to Contractors
 - Discontinued DIACAP ATO On-Site Visits
 - Switch to National Institute of Standards and Technology (NIST) Based Requirements
 - Annual Site Visits Replaced with WPS Assessment
 - WPS Executives Attest to Security Posture
 - Can Be Audited Anytime
 - Responsibility Now Ours!
 - Opened Prospect of Improving Internal Processes

Our Opportunity

- Medicare Became Most Comprehensive Audit
 - CMS Minimum Security Requirements (CMSR)
 - Covers All of TRICARE National Institute of Standards and Technology (NIST) Based Requirements
 - NIST /CMSRs Tie Back To DoD/DISA STIGs
 - If We Focused on CMSRs, Results Available for All Audits

Our Opportunity

- Getting More Complex/Time Consuming!
 - With No TMA Monthly Site-CD, Manual Effort Unacceptable
 - Needed More Effective Technology
 - Researched Industry Options
 - Acquired VCM

What is VCM?

- Vanguard Configuration Manager
 - Automated Vulnerability Assessment Solution
 - Assists in Passing a Security Readiness Review (SRR)
 - Tailored to DoD/DISA z/OS RACF STIG Checklist
 - Supports IBM OS/390 and z/OS RACF

VCM Features

VCM Features

Vanguard Configuration Manager



Includes an interview process for data collection, an automated data analysis process* and summary-level and detail-level reporting*



Speeds the data collection process by ensuring that your answers are saved across checks that require the same data



Saves the answers for each interview question so you don't have to recollect the information required for subsequent reviews

*Available online and in batch







VCM Benefits



VCM Benefits

Eases the requirements of a SRR by automating the step-by-step procedures or instructions of the Checklist

-  Once data has been collected for the target system (a process that takes only a few days of work, at most, the first time), the target system can then be analyzed on a continuous basis
-  VCM looks at live data when possible on the target system
-  VCM goes into great detail providing the end user with the rationale of both FINDINGS and NO FINDINGSs against the STIG checks
-  Without VCM the process of complying on a SRR STIG Audit will take months of man hours and will more than likely be incomplete and inaccurate

VCM Benefits

INFORMATION
SECURITY
EXPERTS

VCM Benefits

VCM automatically determines if a FINDING exists



There is no interpretation of the STIGS required by the user



VCM provides enhanced compliance checking. Example: When looking at dataset profiles, the STIGS make no mention of the GAC and warning flags. VCM is smart enough to look at all relevant configuration controls and test them.



Anyone with basic knowledge of the system configuration can execute and create an Security Readiness Review of the DISA STIGs report






VCM Phases

VCM Phases

INFORMATION
SECURITY
EXPERTS



1. Getting Started


-  Overview of Phases
-  Working with VCM datasets
-  Filtering

2. Common Configuration






3. Collection

-  Delta Processing

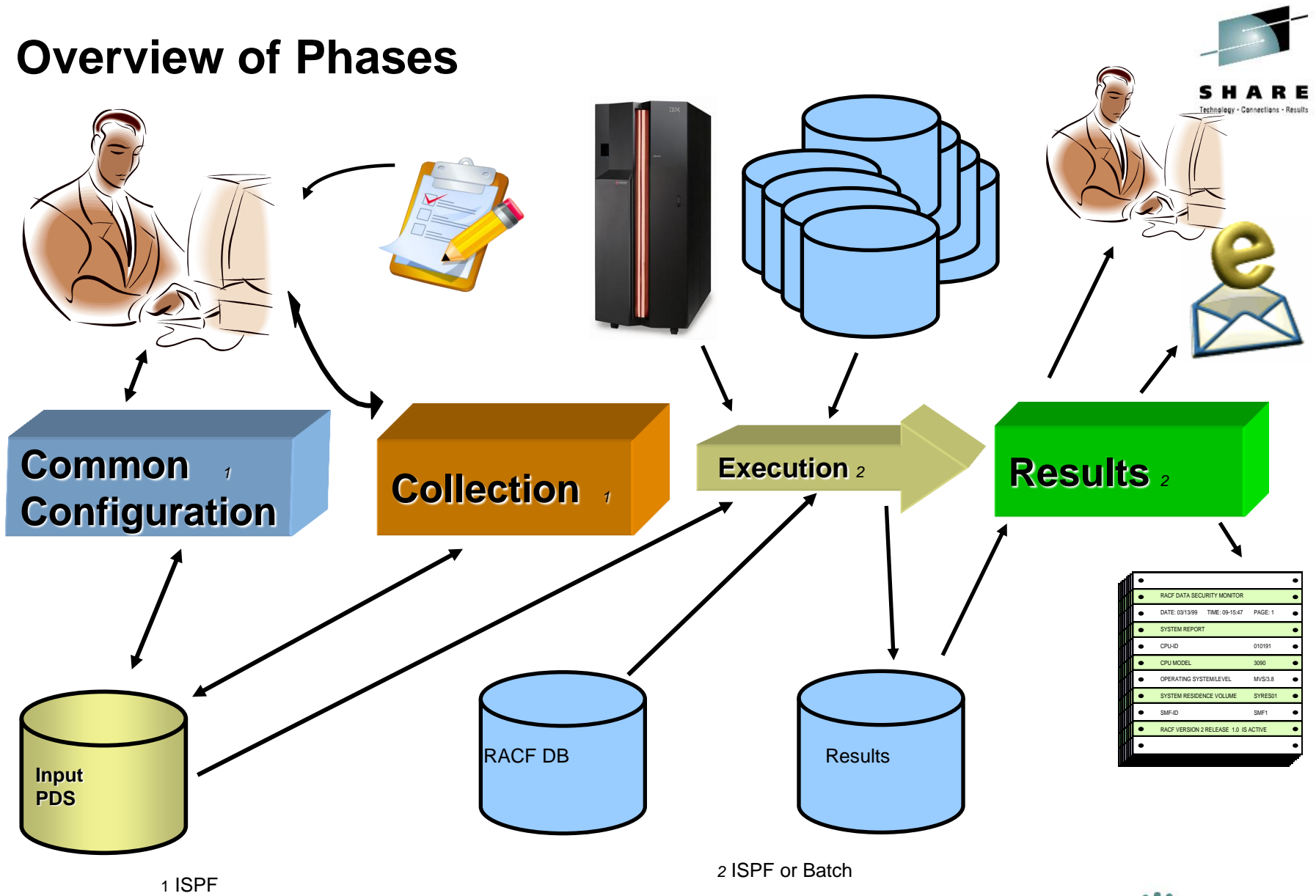
4. Execution

-  Working with VCM datasets

5. Results

-  Working with VCM datasets
-  Filtering
-  Batch Summary & Detail Reporting
-  Emailing and Printing Reports
-  Compare results. You can compare output with current and previous runs of versions of STIGS. Keeps a history of the execution results

Overview of Phases







VCM Phases

INFORMATION
SECURITY
EXPERTS


Phase 1: Getting Started

1. Product Installation

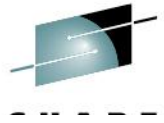
-  Libraries APF Authorized
-  IKJTSOxx member updated
-  VCM LOADLIB LINKLST, STEPLIB or TSOLIB
-  Use VCMSPF or Modify LOGON PROC



2. Review the VCMOPT00 member allocated to the VCMOPTS

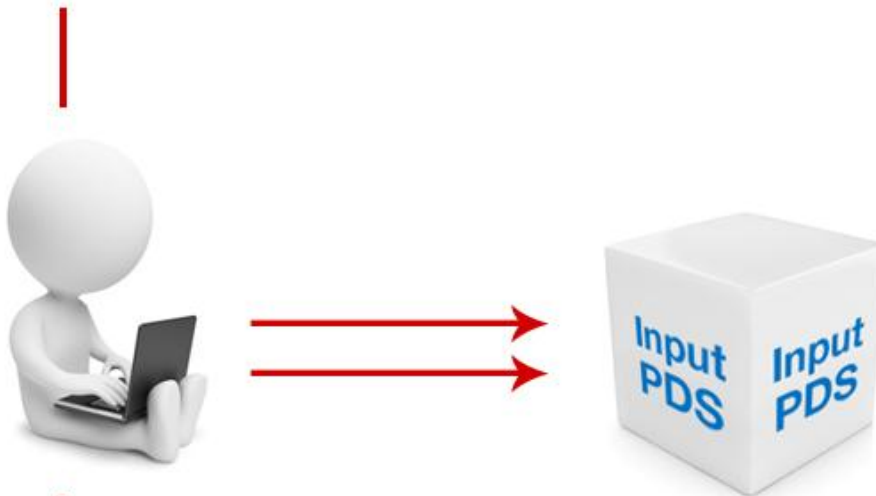
-  Use TSO ISRDDN to find this

2. Interview Preparation Checklist Complete



Phase 2: Common Configuration

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

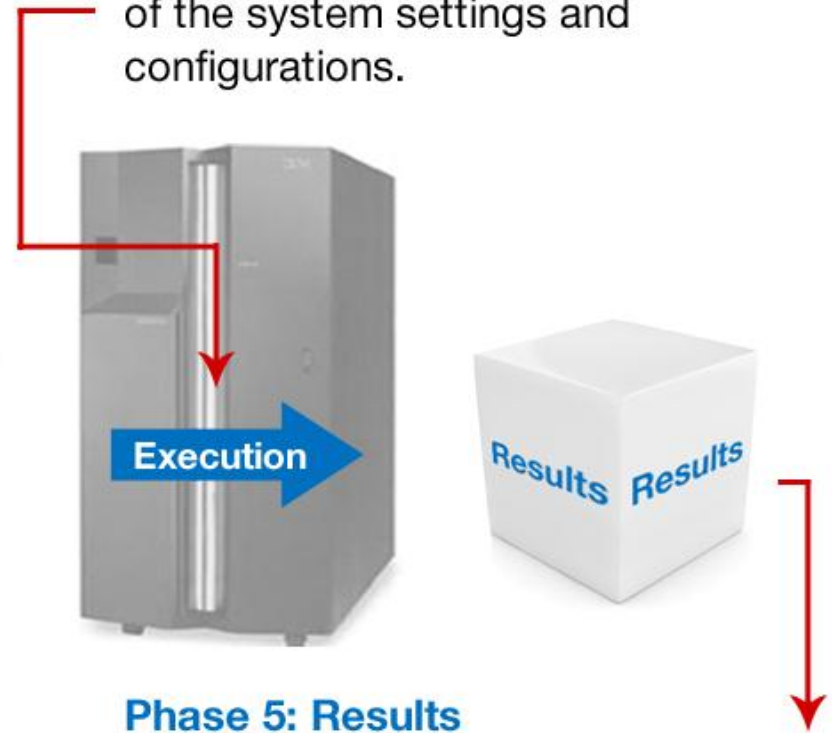


Phase 3: Collection

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

Phase 4: Execution

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



Phase 5: Results

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

Phase 1: Getting Started

INFORMATION
SECURITY
EXPERTS

Phase 1: Getting Started Working with VCM Datasets



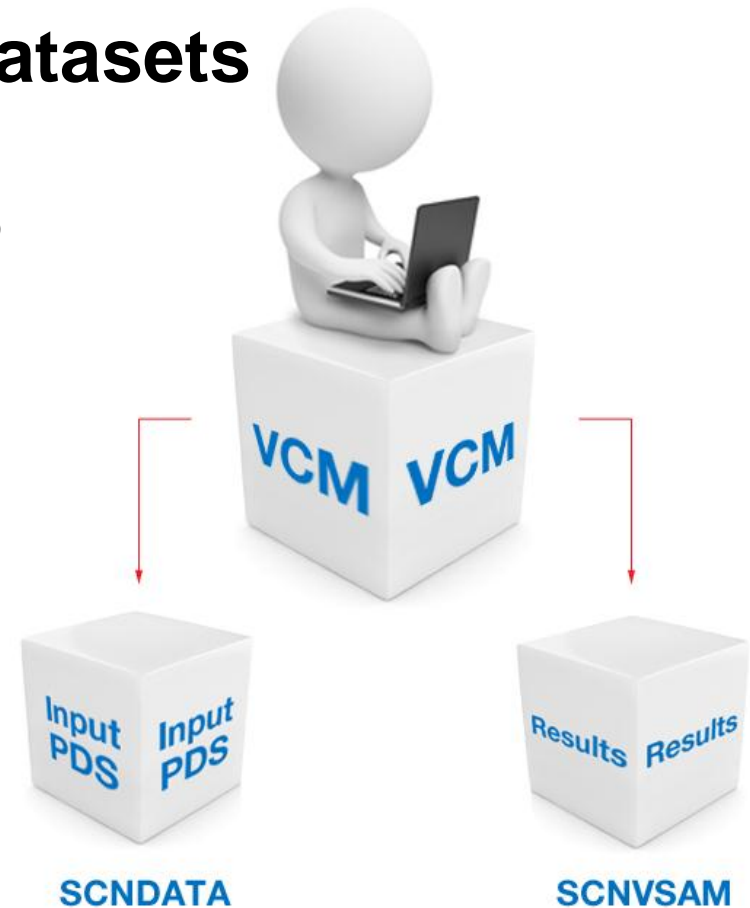
Upon initial entry into the VCM product, you will be asked to select the DoD DISA STIG version to execute, then asked for two dataset names.

SCNDATA data set: Input PDS

SCNVSAM data set: Results



You can switch datasets at anytime by going out to the main screen and selecting the version of checks you want to run.



Phase 1: Getting Started > Filtering

Phase 1: Getting Started Filtering



Filtering is used to exclude categories and/or checks that do not apply to your environment.



Filtered categories and checks will not show up on the VCM ISPF Panels or in the Generated Batch JCL.



A Filter is unique to a VCM user.



Filtered checks will be automatically removed from collection, execution and reporting.



Phase 2: Common Configuration



Phase 2: Common Configuration

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

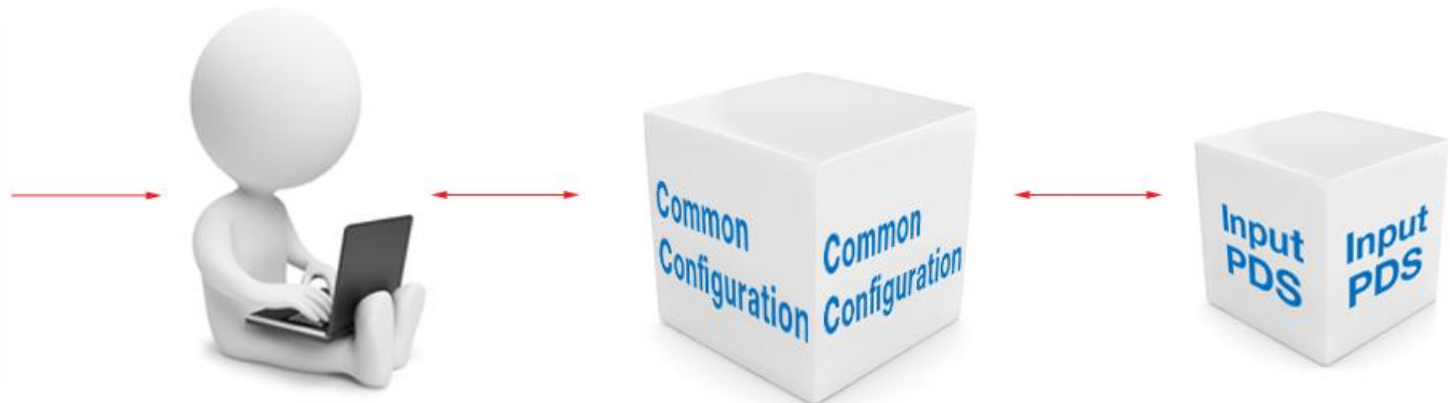
From the DISA STIGs Version

6.9 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



Phase 3: Collection



Phase 3: Collection

Collection can be done on a single check by placing a 'C' next to the check; and for multiple checks, 'Cxx', where xx is the number to collect



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 effect on the Common Configuration Member. This is referred to as Delta Processing.







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

Phase 3: Collection

INFORMATION
SECURITY
EXPERTS

Phase 3: Collection

-  Some data input is optional. This will be reflected on the panel stating: If request is not applicable, leave input field(s) blank.
-  Extensive online help is available.
-  Once data is collected it will indicate who collected it and when
-  Data collection by default is forced again after 30 days. This is controlled by the DAYS_VALID parameter in the VCMOPT00 member



Phase 4: Execution

Phase 4: Execution

During Execution of the checks, VCM 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.

Phase 5: Results



Phase 5: Results

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, i.e. RACF0480-04N

Our Experience – ‘The Old Days’

- TRICARE - DIACAP ATO Process
 - Very Time Consuming
 - Used CA-Examine and SRR Scripts for 6 LPARs
 - Additional Week to Understand/Resolve Findings
 - Consumed Staff of Over 15 Techs and Security Staff
- Medicare Efforts Duplicated/Convolutated Effort
- High Risk of Missing Mitigation Requirements
- Potential Adverse Impact on Contracts/Future Business

Our Experience – Today

- VCM Runs Concurrently on All LPARs
 - 1-2 Hours Total
 - Findings Are Immediate and Clearly Described
 - Now Run Weekly for Proactive Scanning
- Reports Sent to Administrators For Resolution
 - Mainframe System Programmers
 - IT Security Personnel
 - Imported to Internal Central Vulnerability Data Base
 - Combined with Multi-Platform Reporting

Our Experience – Today

- Quarterly Submission Requirements Easily Met
- High Confidence Levels for TRICARE/Medicare Needs
- CMS May Require Monthly Scans
 - Not Possible with Old Method
 - Can Do Easy With VCM
- Reduced Staff Involvement from 15+ to 3
 - Old Process Required Manual Reviews
 - VCM Tailored to DoD/DISA STIGs
 - Reviews Automated

Our Experience – VCM Acquisition

- Internal Proof of Concept
 - Two Trainers for a Week
 - Installation/Configuration/Collection Very Smooth
 - Outstanding Results!
- Acquired/Continued Running
- Superb Support Since
 - Problems Fixed Within a Week
 - Some Immediate
 - New STIGs Supported Within a Month or Less
 - Updates Come as Single SMP/E PTF

Wrap-Up

- Government Security Requirements Complex!
- Getting More So
- Lack of Appropriate Technology Costly
 - Staffing
 - Loss of Contract
 - Future Business Unlikely
- VCM Put WPS in Proactive Position
 - Minimized Staff Impact
 - Improved Security Posture
 - Well Positioned for Upcoming Changes

Wrap-Up

- Government Security Requirements Complex!
- Getting More So
- Lack of Appropriate Technology Costly
 - Staffing
 - Loss of Contract
 - Future Business Unlikely
- VCM Put WPS in Proactive Position
 - Minimized Staff Impact
 - Improved Security Posture
 - Well Positioned for Upcoming Changes