Vanguard Configuration Manager

Vanguard Configuration Manager™ automates the difficult and time-consuming process of testing mainframe security configuration controls to assess their compliance with the z/OS and RACF® configuration checklist from the National Checklist Program (NCP) of the National Institute of Standards and Testing (NIST) and the Department of Homeland Security (DHS).

U.S. government agencies and contractors with IBM® z/OS systems are mandated by the Federal Information Security Management Act (FISMA) to follow applicable NCP checklists.[i] Since August 27, 2010, the NCP recognizes the Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIG)[ii] as the security configuration controls for z/OS and RACF systems.

In addition, Gartner recommends that all organizations with z Series systems use the DISA STIG for z/OS and RACF for internal risk assessments.[iii]

Reduces DISA STIG Assessment Costs

Configuration Manager was designed to provide the fastest, most cost-effective and accurate method to verify that security configuration controls are in accordance with the DISA STIG for z/OS systems.

Vanguard's team of United States-based, z/OS mainframe security experts analyzed all of the DISA STIG z/OS and RACF checks to determine how best to interpret them, test configuration controls for compliance and report findings. This comprehensive intelligence was built into Configuration Manager along with efficient automation capabilities.

The result is that organizations using Configuration Manager can perform System z checks and report findings in a fraction of the time of standard methods. Configuration Manager also allows organizations to easily move to continuous monitoring from periodic compliance reporting.

Improves DISA STIG Test Processes

Verifying that mainframe systems are in accordance with the DISA STIG can require that more than 300 checks be performed, depending on specific configurations.

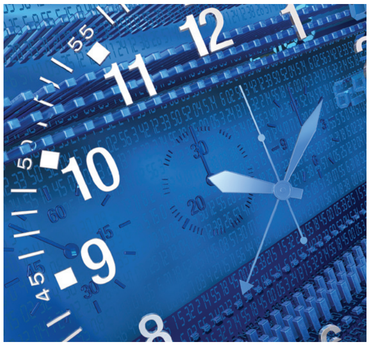
For each check from one to hundreds of thousands of control points must be tested.[iv] It can be extremely costly and time consuming to use standard processes to verify that z/OS systems are configured correctly, even for smaller installations.

Organizations that use standard processes to comply face the following challenges:

- Configuration checks take too long or are impossible to complete.
- Team morale is negatively impacted by the added workload.
- Multiple findings for the same checks are common.
- Ambiguous checks can put teams at risk if interpreted incorrectly.

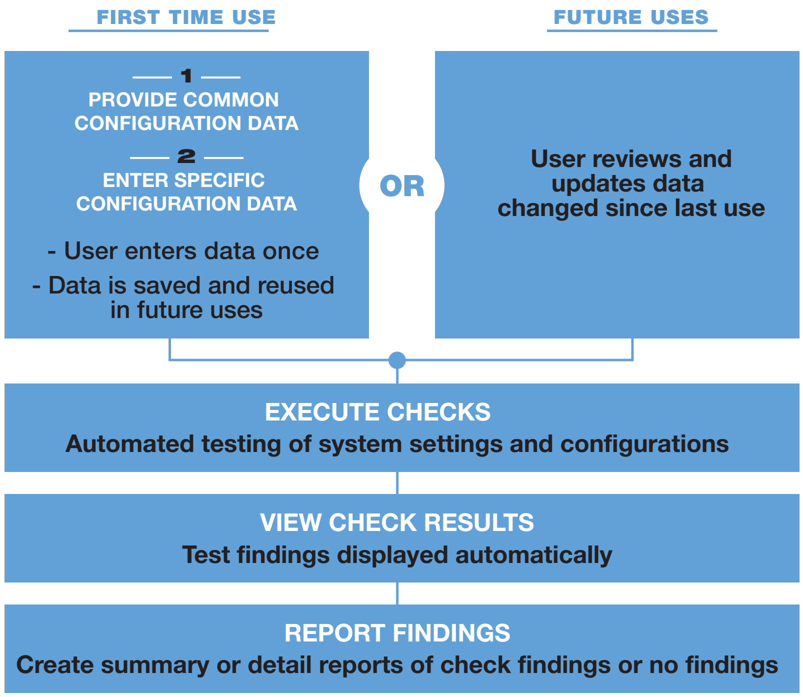
With Configuration Manager, organizations can perform tests and report findings in a few hours each quarter, instead of the hundreds, or thousands, of hours required when using the standard z/OS DISA STIG Checklist process.

Once Configuration Manager has identified findings, they can be remediated, as required, to improve an organization's overall z/OS security baseline and increase security levels.



- **Dramatically reduces costs of configuration control testing and reporting based on NIST/DHS standards.**
- **Significantly enhances z Series security.**
- **Provides built-in intelligence about z Series configuration control details.**
- **Automates testing on more than 300 z Series configuration control checks.**
- **Produces accurate compliance reports in minutes.**
- **Enables implementation of continuous monitoring.**
- **Easy to deploy and use.**
- **Reduces human error in the compliance checking and reporting process.**
- **Developed by security experts in the United States.**

How **Vanguard Configuration Manager** Works


FIRST TIME USE
FUTURE USES
1
PROVIDE COMMON CONFIGURATION DATA
2
ENTER SPECIFIC CONFIGURATION DATA
- User enters data once
- Data is saved and reused in future uses
OR
User reviews and updates data changed since last use
EXECUTE CHECKS
Automated testing of system settings and configurations
VIEW CHECK RESULTS
Test findings displayed automatically
REPORT FINDINGS
Create summary or detail reports of check findings or no findings

In addition to meeting all reporting needs, Configuration Manager is extremely easy to deploy and use, streamlines information gathering and input processes, automates checks and testing, is self-documenting, and provides flexible reporting options.

About Vanguard Integrity Professionals

Vanguard Integrity Professionals, an IBM Business Partner, provides enterprise security software and services that solve complex security and regulatory compliance challenges and deliver a rapid return on investment. With automated solutions for Audit and Compliance, Operational Security and Intrusion Management, Vanguard enables government agencies and corporations around the world to ensure continuous monitoring of z/OS systems, safeguard cloud computing secure domains, and protect critical data and applications from cybersecurity threats.

For More Information

To learn more about the features and benefits of Vanguard enterprise security solutions, visit www.go2vanguard.com or call (702) 794-0014.

TECHNICAL FEATURES

- Creates summary and detailed reports to provide the proper information required.
- Builds and maintains a file with the information required for each environment.
- Executes in both batch and online environments.
- Supports parallel collection and execution of checks to enable reporting to be completed quickly.
- Architected to prevent failure of one check from affecting reporting on another check.
- Consistent look and feel across all DISA STIG categories.
- Users do not need to be an expert on the DISA STIG to complete checks and report on compliance.
- Supports mainframe DISA STIG versions 6.4, 6.5 and above.
- Current release supports z/OS RACF; upcoming releases will support z/OS ACF2 and z/OS TSS.

www.go2vanguard.com