z/Assure® Compliance Assessment Manager™

Frequently Asked Questions

Q: What is z/Assure CAM?

A: z/Assure CAM – Compliance Assessment Manager (CAM) is an automated configuration based vulnerability assessment solution that assists organizations in passing a Security Readiness Review for a z/OS mainframe environment with RACF, CA Top Secret or CA ACF2 as the ESM.

Q: How does z/Assure CAM work?

A: z/Assure CAM uses a Machine-Readable Security Policy (MSRP) to compare expected results in the MSRP to the actual results on the system and reports on any differences found.

Q: What is a Machine-Readable Security Policy?

A: A Machine-Readable Security Policy is a file that is read by z/Assure CAM. The Machine-Readable Security Policy is made up of one or more checklists. Each checklist is made up of one or more checks. A check is made up of one or more penetration tests and a penetration test is either a manual test, a settings test, or an excessive access check.

Q: What is a Checklist?

A: A Checklist will cover a functional area of z/OS or an ISV product. The Checklist is intended to ensure that the configuration and security for the area covered by the Checklist has been performed to the set of standards defined in the Security Policy. The collection of all Checklists represents the installations Security Policy for that system. The Security Policy is represented by the MRSP.

Q: How is a Machine-Readable Security Policy created?

A: z/Assure CAM is delivered with a pre-built MSRP that implements the current DISA STIG standards. The MSRP is configurable by the customer to add their own checklists, checks, and penetration tests pertinent to their organization and to disable existing checklists, checks, and penetration tests that do not apply to their organization.

Q: Is it possible to share a Machine-Readable Security Policy between two or more systems?

A: Yes, the MSRP can be shared between systems minimizing the potential MSRP configuration updates required by the customer.

Q: What are some of the benefits of z/Assure CAM?

A: z/Assure CAM benefits include:

- Significantly reduces the time, effort, and personnel required to perform an audit or Security Readiness Review (SRR).
- Provides a security policy that can be customized to your own regulatory and/or audit requirements.
- Reports compliance findings for remediation
- Ease of installation and ease of use
- Repeatability providing consistent results

Q: How often should z/Assure CAM be run?

A: Initially it is expected that z/Assure CAM will be run 'on demand' until compliance with the installations Machine-Readable Security Policy is achieved. Once compliance has been achieved, KRI recommends that the execution interval be daily.

Q: How are excessive access checks performed?

A: z/Assure CAM requires the installation to assign users to pre-existing and/or customer defined Roles in the MSRP. MSRP Checks specify that a Role has a certain access to a protected resource. z/Assure CAM compares the users authorized (via a Role) with actual users permitted access via the ESM. Users that have access via the ESM but not via the Role will be flagged as having excessive access.

Q: What types of reports does z/Assure CAM provide?

A: z/Assure CAM provides two types of reports, a Summary Report, and a Detailed Report.

The Summary Report has two versions, a Summary Statistics Report, and a Summary Detail Report. The Summary Statistics Report is a subset of the Summary Detailed Report and provides a pass/fail indication for each checklist that was executed. The Summary Detailed Report contains the information in the Summary Statistics Report and in addition provides a pass/fail indication for each check that was performed. The Summary Reports are most useful once compliance with the MSRP has been achieved to quickly determine if the system is still in compliance.

The Detail Report provides detailed information for any errors. Errors may include failing checks but may also include required MSRP customization that has yet to be completed. The description of the message provides information on what needs to be done to correct the error.

Q: Doesn't the MSRP just duplicate my ESM database?

A: No, the MSRP defines the installations security policy and the ESM database defines the installations security implementation. The MSRP is the set of golden rules that the ESM should implement.

Q: Who maintains the Machine-Readable Security Policy (MSRP)?

A: The organization should create a group of knowledgeable individuals that are responsible for maintaining the MSRP and deciding the corrective actions that should be taken when z/Assure CAM discovers a finding. KRI refers to this group as the Compliance Review Committee (CRC). The reason a separate group (the CRC) addresses the findings is that the corrective action may be to update the MSRP or to update the security implementation on the system.

Q: What are the system requirements for z/Assure CAM?

A: The following system requirements must be met to install and run z/Assure CAM:

- z/OS 2.1 and above
- A SORT program must be available without requiring a STEPLIB DD statement and it must be named SORT.
- Library for REXX on zSeries (5695-014) or the REXX Alternate library support must be available
- The Catalog search interface is used by z/Assure CAM. All catalogs might be searched, therefore any issues with your catalog structure must be repaired prior to running z/Assure CAM.