CA Top Secret® for z/OS

Best Practices Guide

r15

Second Edition

CA Technologies Product References

This document references the following CA products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Audit
- CA Audit for z/OS (CA Audit)
- CA Cleanup for CA Top Secret® (CA Cleanup)
- CA Compliance Manager for z/OS (CA CM)
- CA Chorus™ Software Manager (CA CSM)
- CA PAM Client for Linux for System z (CA PAM Client)
- CA Security Command Center (CA SCC)
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Best Practices Guide Process

These best practices are based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are a collaborative effort stemming from customer feedback.

To continue to build on this process, we encourage you to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best *practices, c*ontact us at techpubs@ca.com and preface your email subject line with "Best Practices for product name" so that we can easily identify and categorize them.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- SECCACHE (see page 22)—Removed a consideration regarding using the TSSFAR utility SFSTATS. The consideration does not apply to the SECCACHE control option.

Contents

Chapter 1: Installation Best Practices

This section contains the following topics:

Pre-Installation Information

We recommend that you gather essential installation information before starting the installation process.

Business Value:

By gathering all of this information prior to installation, you can expedite the procedure.

Additional Considerations:

The following information is required during CA Top Secret installation:

- The approximate number of present and future zones, divisions, departments, users, and profiles that you plan to define to CA Top Secret
- The number of present and future DASD volumes CA Top Secret will manage
- The owner of CA Top Secret security and recovery files, which is usually the Master Central Security Administrator (MCSA)
- The security file key, which you need to read an existing security file

More Information:

For more information about product setup, see the *Installation Guide*.

CA CSM

Use CA CSM to acquire, install, and maintain your product.

Business Value:

CA CSM provides a web interface, which works with Electronic Software Delivery (ESD) and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install CA Top Secret.

CA CSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA CSM to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Considerations:

After you install the product, use the CA Top Secret documentation set at http://ca.com/support to configure your product. CA CSM can continue to help you maintain your product.

More Information:

For more information about CA CSM, see the *CA CSM User Guide*.

Chapter 2: Initialization Best Practices

This section contains the following topics:

Modifying the Started Task

We recommend that you implement proper update controls to ensure that a user does not modify the CA Top Secret started task procedure without authorization.

Business Value:

You must modify the CA Top Secret procedure (TSS) to specify several data sets that CA Top Secret uses. Proper update control of the CA Top Secret procedure is important because it defines many critical configuration elements, including:

Security file

Identifies the primary encrypted security file consisting of the security records that contain all user and resource permissions and restrictions. When a user initiates a job or signs on to an online facility in a z/OS environment, CA Top Secret obtains the user's security record from the security file, and places it in the user's address space for the duration of the session.

Backup Security file

Stores the automatic daily backup of the security file to ensure complete integrity of the security environment. The backup file is an exact copy of the security file as it existed at the time of last backup. You can use this file if the device containing the security file becomes unavailable.

Parameter file

Stores and defines control options at initialization and sets up the CA Top Secret operating environment.

Audit Tracking Files

Store security incidents in place of, or in addition to, SMF. The audit tracking files provide administrators and auditors with a current, online record of system security activity from all CPUs.

Additional Considerations:

Because CA Top Secret starts as a subsystem, the CA Top Secret started task procedure must reside in the SYS1.PROCLIB data set or in any data set within the SYS1.PROCLIB concatenation.

When properly installed, CA Top Secret initialization routines automatically define the CA Top Secret subsystem definition during the z/OS IPL process. Do not define the CA Top Secret subsystem within any of your site's SCHED*xx* parmlib members because doing so could cause unpredictable results.

More Information:

For detailed information about these files, see *Installation Guide*.

Creating Audit Tracking Files

The audit tracking file is not required to initialize CA Top Secret; however, we strongly recommend you create and implement this file. We also recommend that you place the audit tracking file on the following volumes:

- On a volume that other systems do not use heavily
- On a volume that is not subject to extensive I/O
- On a volume separate from the primary security file

Business Value:

The audit tracking file provides administrators and auditors with a current, online record of system security activity from all CPUs.

Using the audit tracking file instead of System Management Facility (SMF) offers the following benefits:

- SMF recording and reporting can be cumbersome.
- SMF does not provide online display capabilities.
- SMF must be merged from many CPUs for complete reports.

The IBM Health Checker confirms that a conflict does not exist with the placement of the CA Top Secret audit tracking file and the security file, which reduces the number of support issues resulting from performance degradation when these two files share a DASD volume.

Additional Considerations:

The audit tracking file is an online file that records security incidents in place of, or in addition to, SMF.

More Information:

For details about how the IBM Health Checker integrates with CA Top Secret, see the *Installation Guide*.

Creating the Backup Security File

The backup security file is not required to initialize CA Top Secret; however, we strongly recommend that you create and implement this file. We also recommend that you *do not* place the backup file on the same volume, unit, or channel path as the security file.

Note: Do *not* share the backup file between CPUs.

Business Value:

The backup security file is required to use the built-in automatic backup feature to back up the security file. In addition, if the device containing the security file becomes unavailable, you can use this file.

Additional Considerations:

When multiple CPUs share a security file, configure only one system for backup.

Creating the Recovery File

The recovery file is not required to initialize CA Top Secret; however, we strongly recommend you create and implement this file. We also recommend that you place the recovery file on the following volumes:

- On a volume that other systems do not use heavily
- On a volume that is not subject to extensive I/O
- On a volume separate from the primary security file

Business Value:

The recovery file contains an encrypted record of all changes made to the security file. You can use the recovery file to recreate the security file if it becomes damaged or unusable because of hardware or software problems.

Additional Considerations:

This file is a *wraparound* file. When the file is full, recording continues at the beginning of the file, overwriting existing data. The default size recovery file can hold approximately 2,000 changes before a wraparound occurs.

Creating the VSAM File

Beginning with R15, the VSAM file is required to initialize CA Top Secret. We also recommend that you place the VSAM file on the following volumes:

- On a volume that other systems do not use heavily
- On a volume that is not subject to extensive I/O
- On a volume separate from the primary security file

Business Value:

The VSAM file can contain digital certificate, Kerberos, and data classification information that previously was stored in the Static Data Table (SDT). Using the VSAM file improves scalability.

Additional Considerations:

The Virtual Storage Access Method allows the transfer of information between the CPU's main memory and a direct access storage device. Records organized in logical key field sequence, in physical creation sequence, or by relative-record number, can be accessed directly or sequentially.

Starting CA Top Secret

We recommend that you start CA Top Secret as soon as possible during the IPL process. We also recommend that you start CA Top Secret before the Job Entry Subsystem (JES) is active.

Business Value:

Starting CA Top Secret at the earliest possible time during the IPL process helps provide a more secure environment.

Chapter 3: Configuration Best Practices

This section contains the following topics:

Control Options

We recommend that you review and plan how you will configure the CA Top Secret control options. As you plan how you will set these options, we also recommend that you gain a clear understanding of the regulatory compliance laws and regulations that affect your organization.

Business Value:

Control options specified in the CA Top Secret parameter file dictate CA Top Secret processing; therefore, by carefully implementing control options, you can positively affect processing. You can also specify options during startup and dynamically change them using TSS MODIFY commands.

By understanding regulatory compliance laws and regulations, you can implement control options to follow their rules.

Many control options are critical because they can greatly impact how CA Top Secret operates. Control options can also affect performance—poorly chosen or otherwise improper options can negatively impact security processing. They are also critical from a configuration and compliance point of view, especially because each system uses different sources of configuration controls.

Additional Considerations:

After you establish and implement your control options plan, periodically review your control options to confirm that they the configuration is still necessary.

More Information:

In general, using the default values for each control option is the best practice. The following sections detail best practices for control options where the default value is not the best practice. For details about all control options, see the *Control Options Guide*.

CACHE

We recommend that you turn on the CACHE control option. The CACHE control option provides an area of memory for CA Top Secret to place frequently used items from the security file.

Business Value:

The CACHE control option helps reduce I/O and increases system performance. The CACHE control option also allows I/O performed on behalf of one user to benefit another user logging onto a different address space. The IBM Health Checker confirms that you have turned on this control option.

Additional Considerations:

You can determine the recommended value for the CACHE control option by using the TSSFAR utility SFSTATS function. CA Top Secret uses virtual storage above the line within its address space as a method to keep commonly used records from the security file. The CACHE option default is off. Use the TSS MODIFY control option to activate CACHE or specify the CACHE option in the parameter file.

More Information:

For CACHE information, see the *Control Options Guide*. For SFSTATS information, see the *Troubleshooting Guide*. For details about how the IBM Health Checker integrates with CA Top Secret, see the *Installation Guide*.

NEWPW

We recommend that you set the NEWPW suboption MIN to 7. This setting specifies that passwords must be at least seven characters long. We also recommend that you gain a clear understanding of the types of regulatory compliance laws and regulations to which your installation site is subject, and set other NEWPW suboptions accordingly.

Business Value:

Strong passwords are vital to protect your system. Password controls help to ensure that users' passwords are strong enough to prevent unauthorized access to your system and data.

Additional Considerations:

The NEWPW control option specifies when and in what format you can specify new passwords. CA Top Secret includes many options in the NEWPW control option, and you must determine appropriate restrictions for your systems. The strength of and requirements for a site's password policy typically depends on the following:

- Business needs of the site
- Auditor recommendations
- Pertinent compliance law and regulations
- Pertinent industry best practices

The most prevalent compliance regulation that sites face today is the Payment Card Industry-Data Security Standards (PCI-DSS), which sets minimum levels that govern the following:

- Password content
- Password usage
- Password procedures

More Information:

For detailed information about all password options, see the *Control Options Guide*.

OPTIONS

If you are using optional APARs to provide extended functionality, we recommend that you review specified APARs to verify that you need the functionality that they provide. We also recommend that you check if a new control option has replaced the optional APAR.

Business Value:

By eliminating any unnecessary APARs or APARs that we provide as new control options, you can simplify your view of how CA Top Secret is configured.

Historically, we have distributed commonly requested extensions to product operation as optional APARs, which then may become options that you implement by specifying the option number in the OPTIONS control option setting. We have incorporated some of these options into CA Top Secret as control options.

Additional Considerations:

You use the OPTIONS control option instead of applying APARs.

The following list details two examples:

- OPTIONS number 2 is now available as the following control option:

  LUUPDONCE

  Enforces the update of the last-used statistics within the user's security file record once a day following the user's first successful logon.

- OPTIONS number 36 is now available as the following control option:

  INACTIVE

  Specifies the number of days before CA Top Secret denies an unused ACID access to the system after that ACID's password has expired.

More Information:

To review control options, see the *Control Options Guide*.

PDSPROT

We recommend that you use the PDSPROT control option only on data sets that need increased security for its members. If you use PDS member level protection, we recommend that you review the list of protected data sets periodically to address the following points:

- Ensure that valid security requirements exist for each data set listed
- Confirm any changes to data sets
- Confirm that the specified CA Top Secret resource type code does not perform only a blanket allow. In this scenario, you will not reap a practical benefit from activating the additional PDS security controls when security decisions are not being made.

Business Value:

By using the CA Top Secret PDS member level protection facility, a critical CA Top Secret extension to z/OS security, you can extend security to individual PDS/PDSE data set members. You configure PDS member level protection using the PDSPROT control option, which lets you define a list of data sets and optionally the volume on which they reside to be protected.

PDS member level protection is a useful feature, but we recommend that you limit its use to only those data sets needing this tighter degree of security control. Subjecting unwarranted data sets to PDS member level security controls can increase overhead and resource consumption.

Additional Considerations:

Standard z/OS data set security occurs at the data set level only, which means that a user with access to a PDS/PDSE data set also has access to all members within that data set. For most PDS/PDSE data sets, this processing is acceptable because authority can generally be determined at the data set level. However, for critical system configuration data sets such as SYS1.PARMLIB, the security requirements may be more stringent, with different security requirements for different members.

Consider the example of update access to the CA Top Secret, JES2, and other critical system procedures. You may want to employ additional security to ensure that only properly authorized individuals are permitted to update any of these critical members, which is consistent with the change control and update procedures that may be in place.

PWHIST

We recommend that you set the PWHIST control option to at least 4 to prevent password reuse.

Business Value:

This best practice adds an additional layer of password protection by forcing users to use new passwords. Many security policies, auditors, industry standards, and compliance laws and regulations require a password history to protect against password reuse. For example, Payment Card Industry-Data Security Standard (PCI-DSS) v1.2 requires that a user's new password cannot be the same as one of the last 4 passwords.

Additional Considerations:

CA Top Secret offers expanded password history support, which lets you prevent users from using the same password for up to 64 password iterations.

SECCACHE

We recommend using the security record cache (SECCACHE) control option to provide a cache for CA Top Secret to place security records that reflect the status of a user following a system entry request.

Business Value:

The SECCACHE control option helps increase system performance by helping to reduce CPU cycles in the user and security address spaces required to complete subsequent system entry requests. The control option also helps reduce I/O against the security file when the file is shared between systems. The IBM Health Checker confirms that you have turned on this control option.

Additional Considerations:

CA Top Secret manages the cache in a common data space that all address spaces can access.

More Information:

For details about how the IBM Health Checker integrates with CA Top Secret, see the *Installation Guide*.

TSSCMDOPTION

We recommend that you set TSSCMDOPTION to TERSE to improve performance during LIST commands. TERSE does not display the ADMINBY information, ACID hierarchy information beyond the owning ACID, or the full NAME attribute.

Business Value:

This option saves significant overhead in security file access and in CPU time expended.

Additional Considerations:

The TSSCMDOPTION control option lets users establish default settings for TSS command-specific options. The options can be in any order; however, the rightmost takes precedence.

The default setting is VERBOSE, which displays all the related hierarchy ACIDs information beyond the owning ACIDs and the full NAME attributes. If you need the additional ACID hierarchical information or the name attribute to appear on a list, do not specify TERSE.

Resource Access Considerations

For simpler and effective security administration, we recommend that you configure resources in the following manner:

- Set ownership by the appropriate department, division, or zone ACID
- Grant access permission to user and profile ACIDs on an as-needed basis

We also recommend that you do not have profiles own anything.

Business Value:

This practice simplifies administration and avoids unintentional access. In addition, ownership by a profile implies total access to the resource for every user attached to that profile, which is not a secure configuration.

Additional Considerations:

We recommend ownership of a resource by a department ACID for the following reasons:

- Supports safekeeping—the department ACID cannot access the resource.
- Does not imply automatic access to that resource for all users in that department. Each user in that department has to be explicitly authorized to access that resource.

If a department has ownership of many resources permitted many times (over 500), create several dummy departments and split up the ownership. This practice helps improve processing efficiency by balancing distribution on the security file.

Logical CA Top Secret Database Sharing with CPF

We recommend that you use Command Propagation Facility (CPF) password synchronization and extended password synchronization to synchronize critical user password-related fields in complex interconnected environments that employ CA ACF2 and CA Top Secret.

Business Value:

CPF password synchronization and extended password synchronization simplifies administrative procedures and simultaneously tightens security functionality.

All Record Review

We recommend that you review the ALL record periodically to ensure that you are granting access only to resources that *all* users need.

Business Value:

The ALL record contains permits that allow access to all users. Access to resources using the ALL record could unintentionally expose resources and data.

Additional Considerations:

Many resources and data sets are required by all users and therefore should be in the ALL record.

Exit Code Review

We recommend that you implement strict security and change management controls to ensure that only properly certified changes are allowed in the exit code. We also recommend that you periodically review each exit to recertify its applicability and usefulness. If the exit provides a function that this security product now provides, we recommend that you migrate from that exit point to the native product functionality.

Business Value:

Improperly coded exits can bypass security and open your system to exposures. A line-by-line review of exit code can help ensure that exits are performing their intended function. As this security product continues to grow, we have added exit functionality to the base product, typically using new options, security records, privileges, and so on.

Additional Considerations:

The CA Auditor freezer function can you help you automatically monitor this critical data.

In addition, CA Health Checker validates all CA ACF2 security exit points as well as checking that JES2 exits are in place and enabled.

Securing Linux on z/OS

If your installation is using mainframe Linux, we recommend that you use CA PAM Client for Linux for System z (CA PAM) to secure mainframe Linux signon processing. The Pluggable Authentication Module (PAM) integrates with external security managers such as CA Top Secret and CA ACF2 to extend your existing security implementation to Linux for System z.

Business Value:

This best practice offers the following benefits:

- It simplifies mainframe Linux administration by eliminating the need to define user credentials on the Linux platform itself.
- It helps enforce your existing security policy, enabling you to greater leverage your investment in CA Top Secret and in administrative processes and controls.
- It extends mainframe CA Top Secret reporting capabilities to include mainframe Linux signon activity.

Additional Considerations:

By eliminating native Linux user directories and using CA PAM, you can secure mainframe Linux signon processes through user credentials that CA Top Secret maintains.

Securing z/OS UNIX

We recommend that you employ a single standard security model covering both z/OS resources and UNIX resources.

Business Value:

The SAF HFS security feature lets CA Top Secret bypass z/OS UNIX security access validation. CA Top Secret then secures z/OS UNIX using familiar tools, procedures, and processes. This familiarity helps improve end user efficiency and can limit errors.

Additional Considerations:

Today's z/OS system is actually a merger of two discrete operating systems—the traditional mainframe MVS operating system and the UNIX operating system. Most elements of both are merged into a single, cohesive package, but security remains two separate security models—the traditional mainframe MVS security model and the traditional UNIX security model.

For security administration of z/OS UNIX, the default UNIX method does not provide the same granular control that CA Top Secret HFS security provides. In addition, HFS security is maintained using the same procedures as used for traditional z/OS resources.

SAF HFS security is an application of event notification facility (CAIENF) and UNIX System Services (USS). This security application activates when the appropriate Data Control Modules (DCMs) are linked into the ENF database.

More Information:

For detailed background information and the steps to enable this feature, see the *Cookbook*. For information about DCMs, see the *Installation Guide*.

Identifying Cross-System Connectivity Controls

We recommend that you review your overall security enterprise periodically to determine what security relationships exist, if any, between these systems, and how activating any of the CA Top Secret processing options might be beneficial.

Business Value:

Sharing of administrative activity changes can provide considerable benefit in the form of business process simplification through automation. CA Top Secret has control options that enable it to share the following data and resources:

- CA Top Secret administrative commands and password changes with z/OS and VM systems using the Command Propagation Facility (CPF)
- CA Top Secret security file data and command function in a z/OS sysplex environment
- CA Top Secret security file changes with non-z/OS systems using LDAP Directory Services (LDS)
- Password and user ID change information to non-z/OS systems
- Auditing data with CA Audit and CA Security Command Center

Additional Considerations:

Review existing instances of cross-system connectivity in the following ways:

- Ensure that use and deployment is consistent with accepted best practices and your site's security policy.
- Examine remote systems that are connected to help ensure that they are properly secured and that the data provided to and maintained on them is secure. If they are not secure, you must secure them; otherwise, discontinue the remote connection usage until you can properly secure them.
- Ensure that the data being shared is actually being used on the remote system. For example, sending auditing data to a remote CA Audit and CA Security Command Center system when, in fact, the mainframe-provided data is not used on that system can be an issue. You can save processor, administrative, and network overhead by deactivating this remote sharing capability.

Using the Automatic Security File Backup

We recommend that you use the automatic backup feature to protect the security file.

Business Value:

This best practice helps ensure that the backup file is available in the event of a hardware failure.

Additional Considerations:

To use the backup feature, the security administrator or programmer must first create a backup file on an alternate DASD volume. This backup file should reside on a different string with a different control unit than the primary file. This backup file is a copy of the security file; therefore, consider it a sensitive, high-risk data set.

You are required to perform a backup from only one CPU in a multiple CPU environment and activate a backup through one CPU's CA Top Secret parameter file or STC procedure.

More Information:

To manage the automatic backup feature, see the *User Guide.*

Obsolete Digital Certificates

We recommend that you use the SAFCRRPT utility to help identify expired digital certificates or digital certificates near expiration.

Business Value:

This utility can help ease the administrative burden of handling digital certificates.

Additional Considerations:

Before deleting a certificate, determine if you need to renew or replace it.

More Information:

For information about the SAFCRRPT utility, see the *Report and Tracking Guide*.

Removing Obsolete User Definitions and Entitlements

We recommend that you use CA Cleanup to identify and remove obsolete items, such as user IDs and security entitlements.

Business Value:

It is common for a site to have obsolete user IDs and security entitlements. Removing these items from the security file helps provide a more secure system by eliminating items that unauthorized users could exploit to gain access to the system or resources.

Additional Considerations:

CA Cleanup provides automated, continuous cleanup of CA Top Secret security files by monitoring security system activity to identify used and unused security definitions. CA Cleanup identifies access unused beyond a specified threshold and generates commands to remove that access. CA Cleanup also identifies and removes unused user IDs and permissions that each user has but does not use.

Removing Obsolete Controls

We recommend that you implement a control mechanism to validate controls on a regular basis.

Business Value:

Streamlining your security control options and configurations on an ongoing basis is an important part of maintaining proper security controls. By rationalizing your security options and configurations, you are making your system easier to audit, thus making it easier and more cost effective for your compliance officer to confer a satisfactory compliance review.

Chapter 4: Auditing Best Practices

This section contains the following topics:

Logging Controls

We recommend that the security administrator use control options, user-based controls, and entitlement-based controls to control logging based on the business needs of the installation.

Business Value:

Event logging helps ensure that your site enforces policy, but logging does add costs in terms of processing path length, data repository size, and so on. Consider this potential overhead when you determine which logging controls to activate.

Additional Considerations:

Periodically review these controls to ensure that the requested logging controls remain valid and support business objectives, security policy, and site requirements.

The following global control options help you customize when and how you capture data to logs:

ADMINBY

Logs information in ACID security records to indicate the following actions:

- Administrative ACID who performed the change
- Date, time, and system SMFID where the change was performed

LOG

Allows you to note the following actions:

- Identify the types of events that CA Top Secret for z/OS logs
- Specify whether the events are logged onto the audit tracking file, system management facility (SMF), or both
- Specify if the violation message is displayed

The LOG option affects all facilities.

SECTRACE

Activates a diagnostic security trace on the activities of all defined users or of specific users.

By default, CA Top Secret logs failed access attempts. A security administrator can also specify ACTION(AUDIT) in a PERMIT command to cause logging records to be written. In addition, logging occurs when resources that are added to the AUDIT special ACID are accessed.

You can log all activity for a user by using one of the following ACID attributes:

AUDIT

Specifies an audit ACID activity.

TRACE

Activates a diagnostic trace on all ACID activity, such as initiations, resource access, violations, and user security mode.

Consider the role that special privileges play on an individual user level and their impact on logging. CA Top Secret for z/OS generates special log entries based on the following ACID privileges:

NODSNCHK

Specifies that no data set name checks are performed. CA Top Secret for z/OS bypasses all data set access security checks. Auditing occurs.

NOLCFCHK

Allows an ACID to execute any command or transaction for all facilities, regardless of Limited Command Facility (LCF) restrictions. If the NOLCFCHK attribute is in an ACID, that ACID's terminal cannot be locked. Auditing occurs.

NORESCHK

Allows an ACID to bypass security checking for all owned resources except data sets and volumes. Auditing occurs.

NOSUBCHK

Allows an ACID to bypass alternate ACID usage and all job submission security checking. Associated ACIDs may submit all jobs regardless of the (derived) ACID on the job statement being submitted. Auditing occurs.

NOVOLCHK

Allows an ACID to bypass volume level security checking. Auditing occurs.

Regular z/OS System Audit Regimen

We recommend that you constantly audit your mainframe z/OS system by using CA Auditor. We also recommend that you create procedures to audit your physical IT environment.

Business Value:

Regular auditing using CA Auditor offers the following benefits:

- Helps maintain z/OS integrity through timely identification of z/OS customization and modifications
- Helps verify internal compliance to change control procedures
- Minimizes z/OS auditing costs through CA Auditor usage, whether through direct license or through CA Out-Tasking, which is a CA Services initiative whereby customers can engage us to perform regular services

Maintaining the integrity of the z/OS system is necessary to maintain proper system and application functionality. Regular audits can also satisfy many common compliance regulations, laws, and requirements, such as Sarbanes-Oxley (SOX) and the Payment Card Industry-Data Security Standard (PCI-DSS).

Additional Considerations:

As you devise your auditing regimen, consider the following points:

- The z/OS system is the foundation for the applications and data that run your business; therefore, if the z/OS system has integrity exposures, the associated applications have the same exposures.
- A sound security policy bolsters z/OS integrity. Similarly, a proper z/OS implementation supports your overall security because a user could exploit any weakness to circumvent critical security controls and damage your applications.
- Sound system integrity is the result of careful planning, well-defined procedures, proper security and change control mechanisms, and regular auditing to verify that users are following these procedures.

Compliance Auditing

We recommend using CA CM which provides a single source for real-time, compliance-related information and events occurring within the mainframe environment.

Business Value:

CA CM lets you easily manage and audit your mainframe environment. It accomplishes this with continuous, real-time monitoring and collection of compliance and security-related information, policy alerting, and an intuitive reporting interface for compliance and security event reporting. It also gives you the comprehensive auditing tools that you need to prove your compliance to IT and risk-management auditors.

Additional Considerations:

CA CM consists of several components:

- The Change Monitor detects and records changes to external security manager (ESM) configurations, operating system security configuration, and selected PDS/PDSE data sets.
- The Data Warehouse stores information about mainframe security events in a relational repository that is accessible for compliance reporting, allowing complex reporting processes to be initiated. It also provides real-time access to current and historical security information for forensic analysis, going beyond current reporting capabilities of security products.
- The Alert component provides real-time notification of potential security breaches indicated by changes in the security configuration and specific security events. Stakeholders can receive immediate notification of pertinent violations, user activity, and access or change activity to critical resources using email notification, Write To Operator (WTO), or help desk ticket creation.

- The Logger component writes information about mainframe security events to a dedicated z/OS log stream. A historical record of security events is maintained to address compliance and audit requirements and security forensics. This approach provides greater capability and is easier to use than standard log collection using SMF and file-based security journals.
- A web-enabled user interface provides summary and detailed reports that answer the audit question—Who accessed what, from where, and when. For example, you can report on everything a specific user has accessed or everyone who accessed a resource due to a specific permission. From the web interface, you can also create the policy statements that control what events are captured and the actions to take.

More Information:

For a complete description of this product, see the *CA CM Implementation Guide*.

Index