

# Streamlining and Improving Mainframe Security Compliance Management

Carla Flores

MAINFRAME PRODUCT MANAGEMENT

Rana Zayed

MAINFRAME PRODUCT MARKETING

---

## Table of Contents

<b>Executive Summary</b>			
SECTION 1: CHALLENGE	2	SECTION 4: CONCLUSIONS	7
<b>Infusing Efficiencies into Mainframe Security Compliance Management</b>		SECTION 5: ABOUT THE AUTHORS	7
Compliance Is an Enterprise-wide Concern			
Continuous Audit Cycle			
SECTION 2: OPPORTUNITY	3		
<b>Supporting a Culture of Corporate Governance</b>			
Infusing Corporate Governance Policies With The CA Mainframe Security Suites			
Building a Foundation for Mainframe Security Compliance			
SECTION 3: BENEFITS	5		
<b>Realizing a Singular Goal Through Automated and Repeatable Processes</b>			

# Executive Summary

## Challenge

---

The deluge of growing regulatory mandates has created an overlap in priorities and responsibilities for the enterprise compliance and security groups, prompting them to investigate ways that technology can infuse efficiencies. And because mainframes remain an integral part of the data center, the need for streamlined security compliance management extends to that environment.

However, organizations struggle to develop the appropriate tools and processes to lighten the load, which has created excessive redundancies and repetition of manual effort.

## Opportunity

---

Plans for the CA Mainframe Security Suite incorporate integrated and related mainframe security features designed to streamline your regulatory compliance efforts. These include such end-to-end capabilities for policy-based security control, auditing and reporting as:

- Automated checks, maintenance and out-of-the-box reporting
- Monitoring and alerting on user actions and policy violations
- Continual policy refinement
- Security system validation and tools to perform timely remediation
- Review and analysis of history, performance and events

## Benefits

---

These bundled, best-in-class mainframe security products provide a comprehensive platform upon which you can demonstrate effective mainframe security compliance management while positioning yourself for future growth and additional advantages, including:

- Asset optimization
- Process standardization
- Optimization of existing mainframe investments
- Improved mainframe utilization
- Reduced costs

## Infusing Efficiencies into Mainframe Security Compliance Management

Traditionally, security management and compliance management were viewed and tackled as separate, but equal corporate concerns. Security was certainly always an enabler of compliance and compliance was always a driver for security. But beyond that, the areas were addressed in individual organizational silos, where the strategies, tools, and methodologies were fairly slanted and narrow.

With the emergence of corporate governance and the growing body of regulatory mandates, however, the two areas are overlapping and both the compliance and security groups are investigating ways that technology can ease their increasing — and converging — burden. And with as much as 70 percent of legacy data still residing on mainframes, most organizations are finding that the issue is one that crosses platforms.

### Compliance Is an Enterprise-wide Concern

Compliance requirements have become a fact of life for all enterprises — both commercial and nonprofit. From the Sarbanes-Oxley Act (SOX) to the Health Information and Portability and Accountability Act (HIPAA), through the Federal Preparedness Circular (FPC) 65 for governmental continuity of operations (COOP) and the Payment Card Industry (PCI) standard and to North American Electric Reliability Council (NERC) Permanent Cyber Security Standards, mandates with security implications are as pervasive as they are rigorous and specific.

But whereas most organizations have diligently documented compliance policies and procedures and are consistently monitoring the landscape for changes and additions, many are still struggling to implement adequate mechanisms to easily execute on their vast compliance responsibilities.

### Continuous Audit Cycle

Indeed, most have failed to introduce tools and processes to simplify the load and even more lack the monetary and executive support for improvement. Meanwhile, the security and compliance groups grapple to keep pace with the dizzying amount of requests for compliance documentation. If this scenario is eerily familiar to you, you are probably caught in the continuous audit cycle.

The continuous audit cycle is one where you are in an ongoing, reactive state of demonstrating compliance with specific guidelines and governing bodies. While this approach addresses immediate needs, it lacks any real long-term strategy, duplicates effort and usually misses the correlation between good governance and good security management.

And in that “tactical” mode, enterprises are constantly “reinventing the wheel” because there is little or no automation, and therefore, no way to easily identify and address new, applicable and related compliance requirements. What’s more, repeatability, visibility and point-and-click reporting are virtually nonexistent.

*Mainframe security compliance is a journey — and not a final or finite destination — that includes the ability to perform self-audits, secure resources, segregate test and production data and streamline entitlement recertification and validation.*

## Supporting a Culture of Corporate Governance

The key to a more proactive state is in infusing a more comprehensive and integrated approach to mainframe security compliance that provides structure around the full complement of applicable tasks. With such an approach, you can further infuse the spirit and intent of effective corporate governance into your enterprise and create a security compliance foundation that:

- Ensures consistent security processes and policies
- Enables repeatability and auditability of those processes and policies
- Minimizes the effort necessary to demonstrate process and policy compliance with applicable standards

### Infusing Corporate Governance Policies With The CA Mainframe Security Suites

The CA Mainframe Security Suites integrate related mainframe security products into individual packages to ensure optimal value. And if you are one of the many enterprises challenged to streamline your regulatory compliance efforts, the suites provide policy-based security control, auditing and reporting features that help address compliance concerns in your mainframe environment. The suites support the three mainframe external security management packages (CA ACF2™, CA Top Secret® and IBM RACF) in the market today. The components of the suites are:

**CA ACF2™ OPTION FOR DB2 AND CA TOP SECRET OPTION FOR DB2** With a single-point centralized security strategy, CA ACF2 Option for DB2 and CA Top Secret Option for DB2 help you simplify the complex process of managing access to critical DB2 resources, privileges and utilities. This access control solution also provides you with consistent security and logging, coupled with straightforward auditing and reporting.

**CA CLEANUP FOR ACF2™, CA CLEANUP FOR RACF AND CA CLEANUP FOR TOP SECRET®** Fully deployed in a single day, CA Cleanup solutions identify your accounts unused beyond a specified threshold and generate commands to remove unused user IDs, entitlements, permissions and profile and group connections that each user has but does not need. As such, these solutions help you effectively resolve the accumulation of obsolete and excessive access rights that otherwise occurs within a security file over time — a key requirement for compliance with many regulations.

**CA AUDITOR FOR Z/OS** CA Auditor for z/OS (formerly eTrust® CA-Examine Auditing) is an important tool that helps you achieve and maintain compliance with the myriad of regulatory requirements that govern your business and its supporting IT systems. Specifically, CA Auditor helps you plug a significant hole in the z/OS operating system with comprehensive auditing, integrity check and verification capabilities. It gathers and displays system hardware and software information, analyzes system customization variables, reviews executables, inspects programs, facilitates baseline security configuration, monitors file usage, makes suggestions, answers questions and more. CA Auditor supports mainframe security databases in the CA ACF2, CA Top Secret and IBM RACF environments.

**CA WEB ADMINISTRATOR FOR CA ACF2™ AND TOP SECRET® FOR Z/OS** To help you address the limited, text-based options for maintaining your z/OS security information and the voids you are feeling from the retirement of knowledgeable security administrators, the CA Web Administrator provides a Web-based GUI interface to help simplify the management process and function. With the product, all administration is performed in real-time against live CA ACF2 and CA Top Secret data.

### Building a Foundation for Mainframe Security Compliance

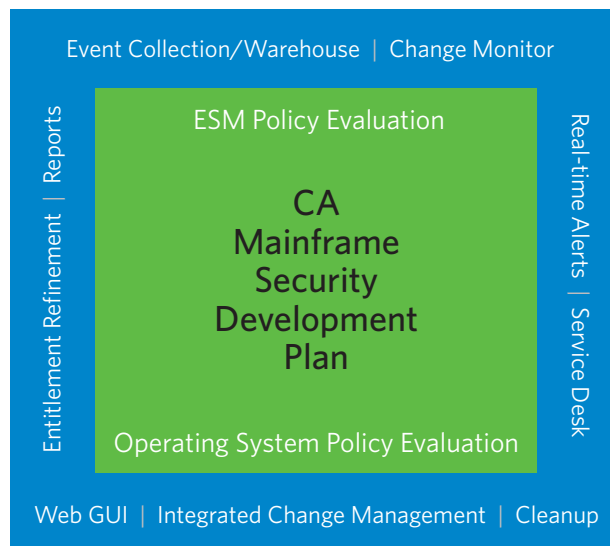
Although, the CA Mainframe Security Suites are already fully featured, they are planned to include additional functionality that is core to enabling security compliance. These capabilities include:

- Change monitoring
- Event history
- Entitlement refinement/cleanup
- Event warehousing
- Intuitive graphical user interface
- Real-time alerts
- Policy refinement
- Forensics
- Comprehensive reporting

FIGURE A

The product development plan for the CA Mainframe Security Suites will allow the bundles to support the policy-based security controls that provide the foundation for security compliance.

### POLICY-BASED SECURITY CONTROLS PROVIDE A PLATFORM FOR MAINFRAME SECURITY COMPLIANCE



## Realizing a Singular Goal Through Automated and Repeatable Processes

The move from a reactive posture to a proactive one that is characterized by automated, repeatable processes for security management is the key to reducing the cost and complexity of compliance. To achieve it, you must go beyond the minimum requirements of regulatory compliance and turn your attention to an organizational governance strategy that affords higher levels of assurance. At a minimum, such a strategy should include the ability to:

- Perform automated checks in advance of auditing
- Validate security system integrity and effectiveness
- Proactively warn of out-of-policy activities to safeguard business information
- Generate reports on a regular basis
- Monitor and alert on events and access
- Continually refine policies
- Minimize human intervention in routine maintenance
- Review and analyze historical events (forensics)

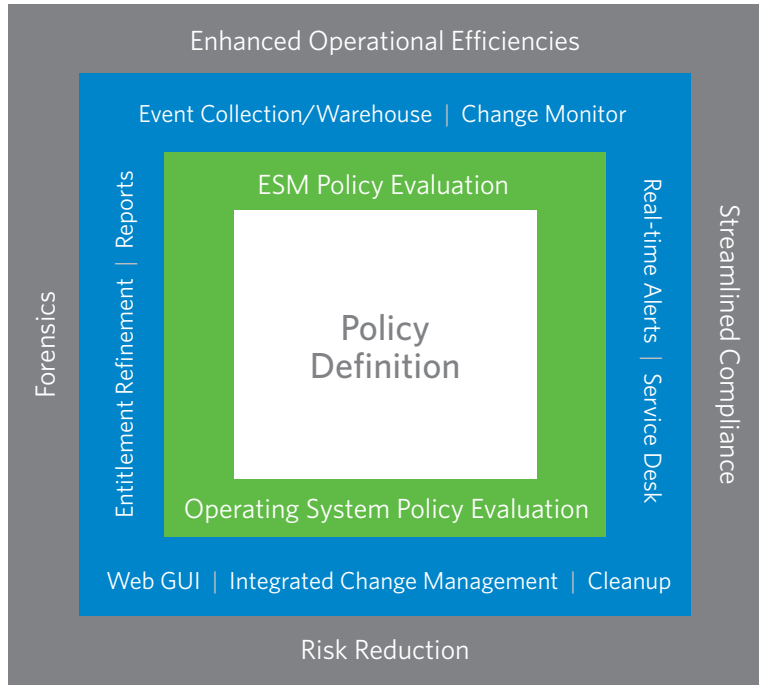
Such a comprehensive approach helps you demonstrate effective mainframe security compliance management, while positioning yourself for future growth and additional advantages, including:

- Risk reduction
- Sophisticated planning via forensic trending and analysis
- Streamlined compliance efforts
- Enhanced operational efficiencies

**FIGURE B**

A comprehensive compliance platform fosters additional improvements through consistent processes.

**DERIVING ADDITIONAL BENEFITS**



---

#### SECTION 4: CONCLUSIONS

The CA Mainframe Security Suites expand compliance support for CA ACF2, CA Top Secret and IBM RACF, helping you identify exposures, validate security system integrity and effectiveness, facilitate proactive notification to safeguard business information and ensure privacy. Centralized management using consistent controls enables efficient analysis and administration of the entire environment, while automated reporting improves staff accuracy and effectiveness, saving time and money.

---

#### SECTION 5

##### **Carla Flores**

Mainframe Product Management

### About the Authors

Carla Flores has more than 15 years experience in the areas of security practices, security policies, security system analysis, user provisioning and business process reengineering. She is currently the Principal Product Manager for Mainframe Identity and Access Management Solutions at CA.

##### **Rana Zayed**

Mainframe Product Marketing

Rana Zayed has spent the past ten years in enterprise software management focusing specifically on the mainframe in the areas of database management and security. She is currently the Senior Product Marketing Manager for Mainframe Identity and Access Management Solutions at CA.

---

To learn more about the CA mainframe security architecture and technical approach, visit [ca.com/mainframe/security](https://ca.com/mainframe/security).

CA (NSD: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

330370608

---

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

