the role of identity and access management in achieving “continuous compliance”

Sumner Blount, Merritt Maxim
CA Security Management
# Table of Contents

## Executive Summary

### SECTION 1
The challenge of continuous compliance 04

### SECTION 2
The lifecycle of continuous compliance 04

### SECTION 3
A platform for unified IT security & compliance 07
- Control identities 08
- Control access 11
- Control information 13

### SECTION 4
Conclusions 15

### SECTION 5
CA content aware identity and access management 16

### SECTION 6
About the authors 17
executive summary

Challenge
There’s a tremendous focus today on complying with regulatory mandates, keeping IT systems secure, and ensuring privacy for confidential enterprise and customer information. And these important business and technology goals are complicated by such factors as increasing regulatory demands, constantly changing IT environments, increasing board and shareholder demands for reduced risk, and the increasing need to reduce compliance costs. An effective and efficient approach to achieving and managing continuous compliance is essential in today’s complex regulatory environment.

Opportunity
There are also business performance opportunities that can be fueled by these new requirements. Effective security controls for compliance can also reduce risk, help to automate key processes for reduced cost and human error, and simplify audits through the automated generation of compliance reports. The core of an effective compliance strategy is a strong and integrated security and compliance infrastructure that protects systems, applications, data, and processes from unauthorized use or access.

However, it’s not enough to just control users’ identities and their access to protected applications and information. To have effective security and compliance, you need to control users’ usage of the data that they have access to. This prevents misuse or disclosure of confidential corporate or customer information.

Benefits
In addition to reaping the benefits of continuous compliance with current and emerging regulations, organizations that employ a unified IT security and compliance platform will be able to:

Reduce risk Protect critical IT and information assets, help maintain privacy of information, and lessen the risk of catastrophic events

Increase efficiency Develop automated and integrated IT and business processes, yielding greater employee productivity and a reduced burden on administrative staff
**The Role of Identity and Access Management in Achieving Continuous Compliance**

Reduce cost Automate compliance processes, eliminate redundancy, and improve productivity.

Improve business effectiveness Improve corporate planning and strategic decision-making, because a strong security and compliance infrastructure enables faster and easier access to corporate information for properly authorized individuals.

Increase business agility Allow the organization to react more quickly to market and competitive events and better take advantage of business opportunities.

Section 1: The challenge of continuous compliance

Leverage compliance for improved business performance

Compliance is often viewed as a burden. But it also presents the opportunity to understand a business more fully, institute effective policies and controls within it, and use these controls and the technology that supports them as a way to enforce policy and improve operations. This is where the real benefits of compliance efforts are achieved. As more companies realize this and leverage their compliance efforts for improved business efficiency, companies that do not adopt this holistic approach will find themselves at a significant competitive disadvantage.

The problem, though, is that many companies have achieved compliance using a “brute force” approach—manual, time-consuming, and error-prone processes that are designed simply to meet the requirements of a given regulation. A more effective approach is to adopt a centralized and integrated security and compliance solution that facilitates continuous compliance across the entire organization. This paper explores the key technologies and best practices that a robust continuous compliance strategy would include.

Section 2: The lifecycle of continuous compliance

There are several key elements of an effective continuous compliance approach. In particular, you need to:

- Define a set of efficient and interdependent phases that interact at key points in the lifecycle and communicate information in a well-defined way.
- Deploy a set of automated security controls that efficiently protect your assets. These should be both preventative controls and detective controls—both are necessary for effective compliance.
- Create an ongoing (preferably automated) process of monitoring all key security controls regularly to confirm they are operating effectively.
- Based on this controls testing, quantify your current risk across all of IT. Based on your risk tolerance levels, you may need to change your existing policies, thereby also strengthening your existing security controls.
Effective compliance is an ongoing, continuous process—a lifecycle of compliance activities. Let’s look at each phase in Figure A in order to identify key activities and technologies that can support and enable continuous compliance.

1. **Identify regulatory requirements** It can be very challenging to understand precisely what the requirements are for a given regulation or set of regulations. Many companies use expensive legal or technical experts who analyze new regulations to determine how to design policies and controls to meet their requirements. The goal is to eliminate redundant controls by mapping all of your regulatory requirements into a core set of harmonized controls that can meet the needs of all of these regulations.

2. **Define policies** Policies are the lifeblood of compliance. A policy is a statement that embodies the goals and behavior norms that the organization wants to instill in its employees and business partners. They are generally determined by regulatory requirements, risks that the company or agency want to control, or the business objectives of the company. Policies are not immutable.
They can change as new regulatory requirements are defined, as the business goals of the company change, or as corporate risk tolerance levels change.

3. **Prevent violations** Preventative controls are used to prevent violations of policy. They are essential for protecting customer privacy, preventing data leaks, and safeguarding access to critical corporate resources such as applications, systems, and information. Technologies such as web access management, privileged user management, and data loss prevention are all essential elements of an integrated approach to preventative security controls.

4. **Detect and correct violations** Not all policy violations can be reliably avoided in all cases. Detective controls need to be established to identify areas of noncompliance so that they can be corrected before the effects become significant. A common example is user accounts that are either dormant (there is an employee owner, but the account is no longer in use) or orphans (owned by a terminated employee). In all cases (particularly the case of orphans), a potential risk exists that would violate the requirements of many regulations and best practices. In this example, procedures could be established that periodically monitor user accounts for these violations and quickly correct them. This could be done manually (a weekly admin scan), but an automated approach (a solution that identifies and terminates these accounts) is more effective and efficient in identifying violations and controlling these potential risks.

5. **Validate controls** The monitoring and validation of compliance controls is a continuous, and often expensive, process. Whether the impetus is from internal audit, external audit, or a regularly scheduled process, controls must be tested in order to validate their correct operation. As best practices have moved towards a risk-based approach to controls validation, controls testing is becoming focused on only testing key controls. This is an important and welcome evolution of best practices for controls validation.

6. **Monitor risk** Compliance should not be done in isolation. It is highly related to, and should be integrated with, a comprehensive program of IT risk management. One requirement is a centralized repository that stores information about controls, risks, assets, regulations, and policies, and maps each object to all related objects. This is the best way to confirm that changes in your compliance profile (e.g., a failed control) also appropriately adjust your current risk profile, which then allows you to take actions to address this increased risk.

Now that we have considered the lifecycle of continuous compliance, let’s look at the key technologies that can be used to provide a comprehensive solution for unified IT security and compliance.
Section 3: A platform for unified IT security & compliance

The need for a unified security & compliance platform

While individual technology components can be deployed to address the most pressing security and compliance requirements, deploying them in isolation can lead to redundancies and inefficiencies that increase cost and potentially increase risk. A comprehensive and integrated security and compliance management platform is the most effective way to assure that an organization-wide compliance effort will be effective, efficient, and sustainable.

The most obvious reason for an integrated platform is that nonintegrated components and disparate systems are generally more complex to administer and manage. Secondly, a unified platform enables the usage of common security elements, policies, and controls across different systems. For example, important security content such as user roles, group membership, data and information classification, and access policies have applicability throughout the organization and across content silos. With a centralized strategy, these policies and controls are standardized so that regardless of which organization, compliance program, auditor, or end user requires the particular information, it is presented in a consistent fashion.

The functions of a unified security & compliance platform

A comprehensive identity and access management (IAM) platform is the foundation of effective security and compliance. The reason is simply that an IAM platform helps you answer the most important compliance questions relating to your users:

- Who has access to what?
- What can they do with that access?
- What can they do with the information they obtained?
- What did they do?

In order to answer these questions, you need to be able to effectively control users’ identities, their access, and their information usage, as follows:

Control identities Manage users’ identities and their roles, provision users for access to resources, simplify compliance with identity and access policies, and monitor user and compliance activity.

Control access Enforce policies relating to access to web applications, systems, system services, and key information. Also, provide management of privileged users to avoid improper actions.

Control information Discover, classify, and prevent leakage of confidential corporate and customer information.
The Role of Identity and Access Management in Achieving Continuous Compliance

Control identities

For most organizations, compliance is not optional. The question is not only if compliance teams need to prove they have adequate controls in place, but how this can be done in the most efficient, cost-effective manner. Automating identity compliance processes, such as entitlements certification or identification of orphaned accounts, means that compliance teams are not continually scrambling to meet audit deadlines.

Identity lifecycle management delivers identity compliance, provisioning, role management, and user activity and compliance reporting (log management) in a modular yet integrated manner. While each function of identity lifecycle management can ease compliance efforts independently, deploying these functions simultaneously delivers considerable compliance efficiencies.

Identity Governance is about implementing processes and controls to facilitate appropriate user access on an ongoing basis. This includes validation processes, such as entitlements certification, which asks users’ managers, role owners, or resource custodians to periodically review and validate...
that current access is correct. Unnecessary access identified through a certification process can be quickly removed to minimize the organization’s security risk.

It can also involve creating a centralized set of security policies to be enforced on a detective or preventative basis to prevent users from receiving or maintaining inappropriate privileges. This includes segregation of duties policies which keep users from receiving potentially conflicting roles or access rights. For example, a user assigned to a role that allows him to create purchase orders should not also have a role that allows him to approve purchase orders.

Entitlements-based reporting is also part of identity compliance, as it helps show who has the ability to do what, so the organization can take corrective action as needed. Implementing identity compliance allows organizations to implement the necessary controls to prevent business and regulatory policy violations while reducing the cost of these validation processes through automation.

**Role management** is a key element of efficiently managing identities and access on a broad scale. Role management tools provide powerful analytics to help organizations build an effective role foundation which includes roles, policies, access rights, etc. Most security-related regulations specify the requirement for a clearly defined process for allocating user access rights. By creating a set of roles that map to job function with a corresponding set of access rules for each role, a set of access rights can easily be assigned to each new user based on his or her role.

The analytical capabilities of role management solutions deliver real compliance value by identifying potential vulnerabilities such as orphaned accounts or over-privileged users. Furthermore, role management solutions can assist in identifying likely roles for each user based on similarities to other users. This improves ongoing role management and allows for compliance processes such as entitlement certifications to be performed more efficiently. Lastly, role management allows organizations to develop cross-system identity security policies which prevent users from gaining conflicting or excessive privileges.

**Provisioning** software automates the processes of on-boarding, modifying, and off-boarding users and their associated access. This type of technology is critically important for regulatory compliance for several important reasons.

First, provisioning helps strengthen internal controls by automating the process of granting and removing access rights. Without some form of automated provisioning, this process is manual and error-prone, and very time-consuming. Also, manual processes are much more difficult to audit than automated ones.

Provisioning also offers powerful preventative capabilities that are important for risk management and compliance. For example, provisioning solutions can check for segregation of duties violations during the user provisioning process to minimize security risk. For example, regulations such as Gramm-Leach-Bliley and Sarbanes-Oxley require strong controls to prevent segregation of duties violations from occurring. These violations exist when a single person can be both the initiator and the approver of a given transaction. Provisioning solutions can also generate warnings when access entitlements being granted to a user are significantly different than those of his/her peers. This is increasingly important
for compliance purposes as organizations seek to reduce the number of “over-privileged” users, as these users can often be a source of compliance violations.

Provisioning also provides an excellent form of “proof” (through audit trails) that the organization followed standard, consistent, and reasonable rules for controlling access to sensitive data. In a compliance audit, it’s generally not enough to merely have reasonable and prudent internal controls in place; you also must be able to “prove it” through a set of reports and audit trails that can be used to validate compliance.

**User activity & compliance reporting (log management)** is one of the most difficult problems in managing the security of a large environment, because of the glut of information about security events that is generated by various system components. Each component often generates its own event and audit log, uses a different format, and reports it to a different location. This flood of information can overwhelm security personnel and make it virtually impossible to really understand the true state of IT security. Massive amounts of data that cannot be acted on intelligently can make monitoring, and thus compliance, very difficult.

Effective compliance requires that there be robust facilities for the logging and reporting of relevant security events, as well as capabilities to synthesize, analyze, and present this information in a meaningful format for administrators. As a counter-example, a system that simply reports thousands of “suspicious” events daily to a log file that is not reviewed or acted on does not represent an effective internal control, and therefore could make a compliance audit much more challenging. The key here is to make the security information actionable and relevant.

Lastly, log management needs to function in the context of a user identity. Knowing that an anomalous activity has just occurred on a critical IT server is no longer sufficient for compliance purposes; that activity must be linked to the given user who completed the action. Through this linking of an identity with an IT activity, compliance lapses and risks can be reduced significantly.

We have seen that a robust identity lifecycle management solution is essential for IT compliance. Identity compliance and provisioning systems help determine which access rights each person has, when and why those rights were approved and assigned, and provides validation that a prudent and consistent policy for management of user access rights is in place. Role management provides a necessary foundation that can identify excessive privileges and potential segregation of duty violations. Finally, user activity and compliance reporting enables efficient monitoring of security controls to improve their effectiveness as well as facilitate compliance.
Control access

The core capability of any IT compliance infrastructure is the control of access to systems and their protected assets (files, applications, services, databases, and the like). Any set of effective internal controls must start with a strong access management component.

There are two broad areas to be considered: web access management and privileged user management. Both are critical for effective compliance.

Any web access management component will include two capabilities: authentication of users and authorization of their access to protected resources. The authentication capabilities need to be very flexible, so that you can vary the authentication method based on factors such as the importance of the resource being accessed, the location of the user, the user’s role, and the like. Also, a range of methods should be available, ranging from simple passwords to biometric methods. Finally, authentication methods should be able to be combined for additional security for certain high-value applications or transactions.

Authorization of users for access to protected applications, resources, and services is a critical element of IT regulatory compliance. A typical example is the requirement in HIPAA to “implement policies and procedures for granting access to electronic PHI [protected health information].” This is a broad requirement, and without a strong authorization management capability, compliance isn’t possible.

Most organizations have to comply with multiple regulations and each may have slightly different authorization requirements, which makes meeting compliance requirements a daunting task. In addition, authorization is often done within each application, resulting in application “silos,” which leads to inefficient and often inconsistent access enforcement. Distributed access enforcement leads to weak internal controls, since administrators will find it hard to determine exactly which access rights any given user has, and how those rights are being enforced across the application suite.

An important capability of access management is Identity Federation. The rapid growth of cloud-based computing and other IT-enabled business-to-business partnerships presents a new set of security management challenges as users attempt to access resources and data across organizational boundaries. Identity federation was specifically created to provide users with secure single sign-on across security domains. As organizations seek to quickly leverage partner-dependent business opportunities, access management systems must support robust identity federation capabilities. It provides a consistent and centralized access management policy enforcement mechanism regardless of whether the use is within the user’s domain or that of a partner’s. Identity federation can also deliver ancillary benefits, such as an improved user experience, reduced development and administrative costs, and improved application security and control of external applications.
One of the most important areas of IT risk relates to controlling the actions of IT and security administrators, called privileged user management. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations, and on the overall security and privacy of corporate assets and information. Therefore, it is essential that admins be allowed to perform only those actions that they are authorized for, and only on the appropriate assets.

Excessive entitlements for admins are also a serious compliance problem. Many regulatory requirements (e.g., PCI-DSS) and best practice frameworks (such as ISO 27001) mandate controls be placed on administrative users. In addition, if a particular access or security violation cannot be traced to a specific individual, it is unlikely that you will be able to pass a compliance audit related to security.

Admins often share (and sometimes lose) their system passwords, leading to an even larger risk of policy violations. And when these users all log in as “Root” or “Admin,” their actions, as reported in the log file, are essentially anonymous. These conditions not only pose a significant security risk, but make compliance extremely difficult because improper actions cannot be prevented nor associated with the offending person.

What is needed is very granular access control on admin users. Unfortunately, native server operating system security does not provide sufficient control over who can access what resources, nor does it provide the granular auditing needed to meet most compliance requirements.

A server access control solution allows systems administrators to create and enforce policy-based controls for user (including privileged user) access to system resources, monitor their activity, and control under what circumstances access is allowed. This provides greater accountability and gives the systems administrator better control of his/her critical resources. An effective server access control solution should protect a wide range of servers and platforms (including virtualized platforms), deliver privileged user management, and provide administrative activity monitoring.

One area of risk is the use of privileged user passwords, which are often set to default values, or are shared with users who should not have these increased privileges. Therefore, Privileged User Password Management (PUPM)—the secure management of privileged user passwords—is a core capability for compliance.

PUPM provides access to privileged accounts through the issuance of passwords on a temporary, one-time use basis, or as necessary while providing accountability of administrator actions through secure auditing. PUPM offers significant compliance benefits not only by restricting access to privileged accounts, but also by monitoring the usage of those accounts. Thus, if a compliance audit uncovers evidence of a potential violation, the host access control tool with its PUPM capability can determine who was responsible for propagating a change on a critical system.
Virtualization Security is increasing in importance as enterprises expand their use of virtual machine technology. By its very nature, virtualized environments pose a special security risk, because if you can breach the hypervisor or another virtual machine, then the amount of damage that can be done is substantial. For this reason, a server access control solution that provides specific protection for the hypervisor, as well as each individual virtual machine, can greatly strengthen your overall security in the virtual environment.

Note that access management capabilities should include any mainframe systems in the environment. Security is only as good as the weakest link, and without effective security for the mainframe, your entire compliance profile is reduced. In addition, integration of solutions across mainframe and distributed systems is important in order to simplify security administration and to enable reasonable consistency of process across the environment.

The access management component of an integrated security and compliance platform thus complements the identity administration component. Once the appropriate users are provisioned and managed, the access management layer can then enforce access to organizational resources based on those same policies. This further strengthens an organization’s IT security and risk profile by facilitating consistency.

Control information

Many identity management providers offer solutions that are focused on managing users’ identities and their access. However, it is critical that information usage also be controlled so that you can determine if anyone is violating usage policies. For example, employees often admit to taking sensitive data out of the enterprise when they leave their place of work or destroying information inadvertently to “make room” due to storage demands. During economic recessionary times, this is a major risk factor that organizations must protect against.

The ability to control access down to the data level (rather than just at the “container level”—e.g., file) is a critical compliance requirement, and one that differentiates major identity management vendors. The term “Content Aware IAM” describes this capability, because the actual content of the data is used to determine if there are violations of security policies. And the users’ history of data usage can be used to dynamically modify their access rights, for example, to help prevent further risks or violations. The ability to dynamically adjust policies and users’ privileges based on their data usage history is an innovative and important evolution of identity and access management.

Organizations need to identify and discover what sensitive information resides across the enterprise and where. Then they must protect and properly control it. This is where Data Loss Prevention (DLP) comes into play.
DLP offers protection against data loss by both analyzing and protecting data on endpoints (laptops, desktops), message servers (internal and external email; mail sent from mobile devices), at the network boundary, and discovering and protecting stored data (e.g., identify sensitive data in SharePoint repositories).

DLP solutions allow for the creation of flexible policies for many types of data (personally identifiable information, non-public information, intellectual property, etc.). Policies inspect data activities for possible security violations. These activities include emailing, IMing, web use, FTP, SMTP, HTTP, saving to removable media, printing files, and more.

The DLP solution can then identify violations and immediately takes the appropriate action, such as blocking an activity, placing it in quarantine, or presenting a warning to the user.

The compliance need driving DLP is obvious. With DLP, organizations can minimize the deliberate or inadvertent disclosure of private or sensitive data. Without DLP, organizations are at risk of data being disclosed, which can lead to compliance violations and their resulting penalties. But there is an increasing business need behind DLP, as customers, partners, and shareholders are expecting organizations to have DLP solutions in place before they’re willing to conduct business with a company. So, a DLP deployment can actually serve as a competitive business advantage.

The last key component of DLP is being able to link sensitive data to an individual identity. It is one thing to know that private data has been accessed and/or leaked; but the real value comes in identifying the user responsible for this action. Once the user is identified, the organization can then examine that given user’s individual roles and entitlements. That examination may determine that the user had excessive privileges, in which case the identity management system can adjust the user’s privileges. But the examination can also identify other users with similar profiles and entitlements and, if necessary, reduce their entitlements as well. Thus, through this process, data can be further protected, and overall risk reduced.

Security and compliance in cloud and virtualized environments

Security in most enterprise environments is a significant challenge. As companies adopt advanced computing models, such as virtualized environments or cloud computing, security becomes even more complex. For example, in a virtualized environment, a breach of the virtual platform can compromise all applications running on all virtual machines on that platform. Similarly, cloud computing offers complex security challenges because of multi-tenancy, with the resulting potential co-location of private corporate and customer information from many cloud clients.

Enterprises have already begun to build out private clouds using virtualization. Virtualized environments demand extremely strong security over the actions of privileged users, because their actions can have such widespread impact. Specifically, granular administrative access control, as well as privileged user management, is essential for securing virtualized environments. In addition, a log management solution can help to centralize and archive security event data from across the virtual enterprise and streamline log analysis and reporting to reduce the cost of establishing IT compliance.
Cloud computing is one of the major new computing trends that require innovative security approaches. Service providers will need to add security to provide assurance to potential customers of cloud-based services. And, because a cloud provider must essentially meet the security and compliance requirements of all of their cloud clients, these cloud-based security capabilities must be robust, standards-based, and rigorously tested. In addition, even if an enterprise maintains its own IT security infrastructure in-house, as it adopts cloud services for some capabilities, it will need to extend its security model to incorporate cloud services. An example might be provisioning users or providing single sign-on to cloud-based services such as Salesforce.com.

Compliance is also more complicated in a cloud environment for two reasons. First, your data may be located at the cloud provider’s site, introducing complex challenges for ensuring that this data remains private and secure, not only from outsiders, but also from other cloud clients and unauthorized cloud administrators. Second, the cloud provider must implement compliance controls that are sufficient to meet the requirements of the regulations that you are subject to. These processes and controls must be tested for effectiveness on a continuous basis, and detailed information should be easily available (through centralized compliance reporting, for example) so that compliance audits can be done without excessive pain or cost.

The key point here is that as you plan your security and compliance strategy and controls, it is important that you include virtualized and cloud-based environments in your planning and design.

Section 4: Conclusions

Security-related governmental regulations generally have many common requirements. The most common ones relate to the concept of knowing who users are, what applications and resources they are entitled to access, and what (and when) they actually have done. The most effective way to achieve this level of control is through a centralized and integrated security management platform that can control identities, access, and information usage.

An integrated security management platform is essential for enabling automated compliance, which facilitates cost efficiencies and reduces the effort required to achieve and maintain compliance. Without compliance automation, the typical manual controls will continue in force, limiting the effectiveness of internal controls and impacting an enterprise’s ability to compete successfully with more nimble competitors.

A comprehensive, content-aware identity and access management platform provides a truly unified approach to the management of IT risk and compliance controls.
Section 5: CA content aware identity and access management

CA is a leading security software vendor who can provide the breadth of capability of a comprehensive and “content aware” security and compliance platform across both distributed and mainframe systems. The components of the CA IAM solution include the following:

**Control identities**

**CA Identity Manager** advanced user management capabilities provide automated user provisioning, user self-service, workflows for managing approvals, delegated user administration, and an easy user interface for creating policies and administering identities.

**CA Role and Compliance Manager** delivers advanced analytics and a powerful policy engine that improve the time-to-value of fundamental activities such as privilege cleanup and role discovery.

**CA Enterprise Log Manager** collects, normalizes, and archives IT activity logs from multiple sources and provides search, analysis, reporting, and alerting capabilities to reduce the cost and complexity of compliance reporting and investigations.

**Control access**

**CA SiteMinder®** provides a centralized security management foundation that enables the secure use of the web to deliver applications and data to customers, partners, and employees.

**CA Access Control** provides a robust solution to privileged user management, protecting servers, applications, and devices across multiple platforms and operating systems. Provides more granular access rights and increased security over basic operating system security. Improves security through the issuance of privileged user passwords on a temporary, one-time use basis, while providing accountability of user actions through secure auditing.

**CA ACF2™ and CA TopSecret® Security** enable controlled sharing of your mainframe computers and data while preventing accidental or deliberate destruction, modification, disclosure, and/or misuse of computer resources. They allow you to control who uses these resources, and provide you with the facts you need to effectively monitor your security policy.

**Control information**

**CA DLP** leverages identity to analyze end-user activity in real time and understand data with a high level of precision to help organizations protect sensitive information more effectively.
Section 6: About the authors

Merritt Maxim has 14 years of product management and product marketing experience in the information security industry, including stints at RSA Security, Netegrity, OpenPages, and CA. In his current role at CA, Merritt is currently director of product marketing for CA’s security and compliance initiatives. Merritt received his BA from Colgate University and his MBA from the MIT Sloan School of Management and is the author of “Wireless Security.”

Sumner Blount has been associated with the development and marketing of software products for over 25 years. He has managed the large computer operating system development group at Digital Equipment and Prime Computer, and managed the Distributed Computing Product Management Group at Digital. More recently, he has held a number of product management positions, including product manager for the SiteMinder product family at Netegrity. He is currently focusing on security and compliance solutions at CA.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies’ innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.
This document shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release, and timing of any features or functionality described in this document remain at CA’s sole discretion. Notwithstanding anything in this document to the contrary, upon the general availability of any future CA product release referenced in this document, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. In the event of a conflict between the terms of this paragraph and any other information contained in this document, the terms of this paragraph shall govern.

Copyright ©2010 CA. All rights reserved. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Intel and Intel Itanium are trademarks or registered trademarks of Intel Corporation in the United States and other countries. Microsoft, SQL Server .Net, Visual Studio, Internet Explorer, Windows Vista, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. Red Hat® and Red Hat® Enterprise Linux® are trademarks or registered trademarks of Red Hat, Inc in the United States and/or other countries. SUSE is a registered trademark of Novell, Inc., in the United States and other countries. Eclipse is a trademark of the Eclipse Foundation, Inc. SPARC is a trademark or registered trademark of SPARC International, Inc. in the United States and other countries. Adobe and Dreamweaver are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Mozilla® and Firefox® are registered trademarks of The Mozilla Foundation in the United States and/or other countries. Solaris is a register trademark of Sun Microsystems in the United States and other countries. IBM, z/OS, z/Architecture, CICS, Sphere, DB2, MQSeries, System p5, System p6, AIX, and DB2 Universal Database are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT WILL CA BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.