

WHITE PAPER

Beyond Compliance: CA Enables the Enterprise to Meet Demands Today, Provides Flexibility for the Future

Sponsored by: CA

Sally Hudson

Rose Ryan, J.D.

March 2007

IDC OPINION

Security concerns abound today, complicated by both internal and external threats and an ever-growing list of mandated compliance requirements. Compliance is now an integral component of everyday business practices. As security and compliance issues merge with business objectives, organizational needs are growing beyond compliance. IDC believes a comprehensive security management solution must be evaluated based on answers to the following questions:

- How does it improve governance?
- How does it reduce risk?
- How does it contribute to streamlining operations?
- How does it enhance and extend identity and access management products?
- How does it align information security with business goals?

Based on the answers to these questions, CIOs, CSOs, and business managers can work together to determine which solutions are best suited to meet the mutual requirements of integrating security management while enabling evolving business goals.

METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. The actual strategy for doing so incorporates information from five different, but interrelated, sources:

- Reported and observed trends and financial activity in 2005 as of the end of April 2006**, information includes reported revenue data for public companies trading on North American stock exchanges (CY1Q04–4Q04 in nearly all cases).
- IDC's Software Census interviews**. IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.

- ☒ **Product briefings, press releases, and other publicly available information.** IDC's analysts meet with hundreds of vendors each year. These briefings provide an opportunity to review current and future product strategies, revenue, shipments, customer bases, target markets, and other key product information.
- ☒ **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain a detailed revenue-by-product-area model for more than 1,200 worldwide vendors.
- ☒ **IDC demand-side research.** This includes thousands of interviews annually and provides a powerful fifth perspective for assessing competitive performance. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

IN THIS WHITE PAPER

Situation Overview

The worldwide Identity and Access Management (IAM) market realized \$3.0 billion in revenue in 2005, IDC anticipates this will reach \$5.1 billion by yearend 2010.

Compliance Today

IDC sees regulatory compliance as the leading driver of IAM market revenue in 2006, and we expect this to continue in 2007. IDC anticipates the overall IAM software market to exceed \$4 billion in revenue by 2009. Additionally, IDC has forecast the authentication token market to reach \$764 million in revenue through 2009 and considers these technologies to be an important measure of achieving IAM compliance within organizations, especially as new form factors are increasingly available to both IT buyers and consumers.

Examples can be seen in the banking and financial industries and all public companies, which have been mandated by the Federal Financial Institutions Examination Council (FFIEC) regulations to provide stronger, more effective forms of authentication, beyond the traditional (and inherently weak) username/password combination. The FFIEC considers single-factor authentication to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

In the wake of recent financial scandals, the Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. Sarbanes-Oxley requires businesses not only to document and assess their internal controls but also to control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by IAM solutions.

Organizations need to address compliance issues surrounding Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), FFIEC, the Payment Card Industry (PCI) Data Security Standard, the Homeland Security Presidential Directive 12 (HSPD-12) policy for a common identification standard for federal employees and contractors, and other federal regulations and guidelines, not only in the United States but globally. Global regulations include the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), Sarbanes-Oxley for Japanese Companies (J-SOX), and the Japanese Personal Information Protection Act (JPIPA). The European Union (EU) Data Privacy Directive by which member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data, Hong Kong's Personal Data (Privacy) Ordinance, Taiwan's Computer-Processed Personal Data Protection Law, and New Zealand's Privacy Act which regulates the collection, use, and dissemination of personal information in both the public and private sectors. There is also Basel II, called "The New Accord" or the International Convergence of Capital Measurements and Capital Standards—A Revised Framework. It is the second Basel Accord and represents recommendations from the Basel Committee on Banking Supervision (BCBS). It was created to promote greater consistency in the ways banks and banking regulators approach risk management across national borders.

These and other federal regulations are prompting enterprises to look increasingly toward identity and access management solutions to help them comply. Compliance with various regulations is manually intensive and, therefore, costly. Enterprises are now seeking to reduce the cost of compliance through automation.

The move from a reactive compliance stance to proactive and cost-effective management is the key to reducing the cost and complexity of compliance. Enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance. The ability to perform automated checks in advance of auditing, to report on a regular basis, and to monitor employees and discern behavior patterns to stop noncompliant actions before they occur requires that steps be taken to achieve proactive and effective cost management.

IDC believes an automated technology solution providing both the security required by the regulations and a way to translate the nebulous regulations into actionable policy and technical controls would greatly save organizations time, thereby saving money.

ID Fraud and Theft on the Increase

Increased incidences of ID fraud and ID theft are also shaping the way businesses look at the IT function today. The news media reports regularly on these events and their impact to businesses, consumers, and even national security. These issues continue to drive legislation for stricter security and stronger enforcements of these regulations in the United States, Europe, and Asia. Industries looking to combat ID fraud and ID theft will want to enhance current IAM solutions and establish best practices for monitoring, maintaining, and modifying these systems as necessary to effectively protect data and information from both internal and external threats.

FUTURE OUTLOOK

Beyond Compliance

Industries are looking to IAM systems to improve in the following areas:

- ☒ **Compliance** with government and industry regulations, and enhanced efficiency around compliance in the United States and other countries
- ☒ **Security** to reduce risks to the organization, especially to prevent identity fraud and identity theft as well as to protect privacy and systems integrity
- ☒ **Auditability**, or who was accessing what information when within the system. Automated auditing and reporting capabilities have become part of the cost of doing business for the majority of organizations worldwide.
- ☒ **Accountability**, which includes access and permission rights as well as who granted these rights and when and why they were granted. The granularity and flexibility required today go beyond simple directory management and are increasingly achieved via provisioning and other IAM products. They are becoming essential to managing and ensuring security in both large and medium-sized businesses.

In conjunction with these criteria, companies also need centralized management and reporting capabilities. Key benefits derived from the deployment of IAM solutions include the ability to automate risk assessment and controls for segregation of duties and shorten the audit and reporting cycles. Tighter integration between IAM functions (e.g., provisioning and single sign-on) and the IT operations (e.g., IT service management and change and configuration) solutions would go a long way to automate the remediation of segregation of duties and the administration and provisioning of access to applications and resources. All of these systems ideally should integrate seamlessly together in a service oriented architecture (SOA) environment.

As a result of having a comprehensive IAM solution, CA is one of the few IT vendors today that can address the above requirements.

CONCLUSION

Increasing regulatory compliance mandates in the United States, Europe, and Asia combined with thwarting ID theft and fraud will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure. A compliance platform includes identity and access management systems and is critical to meeting regulatory standards in many areas, including those in financial, banking, healthcare, government, and pharmaceutical industries.

In order to achieve continuous compliance, enterprises must:

- ☒ Understand relevant regulations and business impact
- ☒ Identify and evaluate existing controls
- ☒ Design new and revamp existing controls to meet common requirements
- ☒ Design processes to enable "proving" compliance to internal and external auditors
- ☒ Leverage compliance as a "platform" or business process that also increases overall business efficiency and effectiveness

Furthermore, IDC recommends businesses adopt a three-point approach to proactively protect the personal and propriety data they hold:

- ☒ Institute and enforce strong security policies for internal employees, outside contractors, temporary employees, and customer interactions and information.
- ☒ Architect and implement strong encryption and security technology to protect networks, systems, servers, and data in transport from unauthorized access.
- ☒ Deploy and rigorously manage a strong identity and access management system to provision, change, and remove user access rights as well as track user access movement from a centralized authorization point. Ideally, this should be built upon the foundation of a centralized, policy-based authorization platform.

CASE STUDY

MasterCard Worldwide

Industry: Financial services, processing services

Location: O'Fallon, Missouri

Employees: Approximately 5,000 staff

Revenue: \$3.3 billion (fiscal year 2006)

Subject: Use of CA Identity Manager within the MasterCard IT environment

Situation Overview

In late November 2006, IDC interviewed Tom Compas, senior business leader, Global Security Solutions, Global Technology, and Operations at MasterCard Worldwide. He describes the IT operations he oversees as "diverse and challenging." Compas manages the identity and access management (IAM) deployment for an organization that includes mainframes, large Unix server farms, HP NonStop servers, Microsoft Windows servers, as well as a significant number and variety of Web servers. Compas' team develops and delivers IAM solutions for MasterCard Worldwide's Global Information Security department, a primary internal business partner.

MasterCard has a very large and diverse end-user community, however, given MasterCard's financial intermediary role in payment processing, much of the consumer-related servicing is conducted via its partner financial institutions.

MasterCard is currently using CA's Identity Manager user administration and provisioning product to automate the accounts and entitlements of its internal staff. The company has a number of other CA IAM solution components, including CA ACF2, which provides access control for mainframes; CA Access Control, which provides access control for Unix and Windows systems; and CA Directory, which provides user directory services. CA Identity Manager is deployed on a series of Windows servers with CA Directory deployed on a pair of Unix boxes.

According to Compas, the selection of CA's Identity Manager was made after an extensive RFP process in the fall of 2004. The selection of CA was based primarily on the company's strong presence in the field and its understanding of the provisioning business. CA also fully understood MasterCard's specific business needs and had the capability to implement a comprehensive solution in a complex environment.

Advantages Gained with MasterCard's Identity Management Deployment

"First and foremost is efficiency," said Compas. The challenge for MasterCard was that its 5,000-person staff equated to approximately 200,000 discreet identities across the organization in different systems. These identities or accounts were managed through a highly varied set of processes, which included manual forms, specialized access databases, homegrown workflow systems, and manually intensive paper trails. "The population of our internal IDs was growing by approximately 30% a year," said Compas, "We had to simplify and automate to keep pace with business dynamics."

By using CA Identity Manager, the company went to a role-based access control model to reduce complexities. This was done by looking at each application individually. This simplified and automated the access control process and mitigated the complexity of the tasks involved.

The second most important advantage gained from the CA provisioning product was increased responsiveness. For example, it used to take an average of 10 days to provision a new staff member with full access privileges. Through enhanced automation, more than 90% of the process is accomplished in a single day. This is a tenfold gain on the provisioning life cycle. Inversely, the process is equally efficient

when someone leaves the company. Departures are communicated to the system through an automatic feed to human resources, and all access is removed immediately from the target systems.

Another benefit of the identity management solution is that the company's HR system is now being used as a single authoritative record of employee status and key information. This helps streamline processes by allowing IT to work with HR to ensure accuracy of data.

MasterCard has always been focused on compliance as a key business principle. The directive of this project was to allow the provisioning systems to complete tasks in a much more efficient and automated manner. The company is now planning to further enhance the system by providing more automation around role management and consolidating reporting into a single repository for all related information.

Finally, another added benefit resulting from this project is increased customer satisfaction. The identity management team has received accolades from all levels of management throughout the organization related to the efficiency gains in the provisioning of employees. New employees are now able to be productive on their first day of employment, as opposed to several days or weeks later.

Resource Requirements For the Deployment

Prior to selecting the CA solution, MasterCard conducted an extensive analysis of the company and its capabilities. CA presented a comprehensive road map for implementing the provisioning product in a rapid but phased approach. At peak times during the rollout, more than 20 people were working on the project. This includes both MasterCard staff as well as experts from the CA team. According to Compas, the successful deployment of CA Identity Manager is essentially complete. Ongoing work requires between 8–10 people across the technology and Global Information Security business group. The business group manages any changes to roles, help desk support, etc. Compas characterizes this as an "advantageous division of duties." The Security Group is the business owner, and the Technical Group is the delivery arm for the solution.

According to Compas, additional maintenance costs associated with introducing, running, and expanding a sophisticated enterprise-scale system will be offset by the reduction of manually intensive provisioning steps by help desk and other administrative personnel.

Challenges Met

According to Compas, one of the greatest challenges to the project was getting people internally to think differently about how identities should be managed and how to accomplish this via a role-based model. MasterCard brought in experts skilled at business process change to help with this endeavor.

"For this project to succeed, it was just as much about the business process change as it was about the technology," said Compas. "This project required a tremendous focus on education and explaining the reasons why we were doing this. We had to demonstrate the benefits of the program to the organization as a whole."

The sheer scale of the project itself was another challenge — a large and complex IT deployment on par with any large-scale ERP implementation. Compas and his team used a formal governance structure for guidance and direction, and found this governance approach to be extremely helpful in the education and communication processes. Key stakeholders were identified across different groups (e.g., business, internal audit, security, etc.) and the team developed a cross-functional panel to review key decisions and provide prioritization and other direction. Major decisions were then subject to an executive review board. This governance structure was formed all with the goal of keeping all involved parties informed and updated as the project progressed.

Conclusion

"We wanted to deliver value quickly," says Compas. The team implemented the Identity Management platform and migrated the first 12 business-critical applications in six months. Through a series of subsequent quarterly releases spanning two years, nearly 200 applications are now under the identity management system.

Malcolm McWhinnie, group head, Global Information Security for MasterCard Worldwide, and the project's executive sponsor, sums it up well:

We are very pleased with the results of this effort. The benefits of identity management are not limited to security administration. We've seen cycle times for provisioning access improve almost tenfold, and we have been able to empower our line managers to really take responsibility for access management [for their people and business applications], without adding a heavy administrative burden. This has created a win-win situation for MasterCard and our managers — a greater business efficiency all around.

APPENDIX

Key Regulatory Drivers

Regulations most often referred to include:

- ☒ **HIPAA.** The Health Insurance Portability and Accountability Act of 1996 requires that to ensure privacy and confidentiality, all patient healthcare information be protected when electronically stored, maintained, or transmitted. It also mandates that each user be uniquely identified before being granted access to confidential information. It specifies that access to personal health information (PHI) be restricted to only those individuals who need access as part of their role.

- ☒ **Sarbanes-Oxley Act of 2002.** In the wake of recent financial scandals, the Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. Sarbanes-Oxley will require businesses not only to document and assess their internal controls but also to control access to financial systems. Section 404 covers internal control activities during the creation of

financial reports and points to compliance risks that can be addressed by IAM solutions.

- ☒ **Gramm-Leach-Bliley.** The Gramm-Leach-Bliley Act mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.
- ☒ **SB1386.** California's Information Protection Act requires companies to report security breaches involving private consumer information. Personal information is defined as social security number, driver's license or California ID card number, account number, credit or debit card number in combination with a required security code, and access code or password that permits access to an individual's financial account.
- ☒ **European Union Data Protection Directive.** Member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data, and individuals' rights concerning their personal data are outlined. This directive is described as the most ambitious and stringent data privacy initiative, and the guidelines to ensure that data is transferred outside the European Union only when it is adequately protected have extraterritorial implications on businesses. The U.S. Department of Commerce worked closely with the European Commission to develop a "safe harbor" framework to enable U.S. businesses to meet EU privacy regulations.
- ☒ **Patriot Act, Title III** (International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001). Section 352 requires financial institutions to develop internal policies, procedures, and controls to guard against money laundering. Institutions are required to track and report suspicious activities and conduct regular independent audits to test antimoney laundering (AML) programs. Additional rules designed to establish a customer identification program also came into effect recently and require financial institutions to document the methods they utilize to verify a customer's identity. A consortium of global financial institutions is looking to define business processes that can be shared between networked members and invoked using Web services and a service oriented architecture (SOA). AML has been identified as one of the key initiatives that would enable member firms to accomplish compliance at a lower cost.
- ☒ **Homeland Security Presidential Directive/HSPD-12** (Policy for a Common Identification Standard for Federal Employees and Contractors). The primary objectives of HSPD-12 are the development and deployment of a federal governmentwide common and reliable identification verification system that will be interoperative between all government agencies and serve as the basis for reciprocity between those agencies. In response to HSPD-12, the NIST Computer Security Division initiated the Personal Identity Verification (PIV) project and established the Federal Information Processing Standard (FIPS PUB 201).

- ☒ **Federal Financial Institutions Examination Council (FFIEC)**-issued guidance in 2001 requiring bank Web sites to adopt some form of two-factor authentication by the end of 2006. Its recommendation carries the force of regulation because banks' failure to comply would earn them black marks from bank examiners. The FFIEC considers single-factor authentication to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

Definitions

Identity and Access Management Products Market View and Definition (IAM)

IDC defines the IAM software market as a comprehensive set of solutions used to identify users in a system (e.g., employees, customers, contractors) and control their access to resources within that system by associating user rights and restrictions with the established identity. This is accomplished via implementation of some or a combination of the following technologies within an organization: Web single sign-on (SSO), host SSO, user provisioning, advanced authentication (e.g., public key infrastructure [PKI]), legacy authorization, and directory services.

These technologies are all critical components of IAM. Further, other elements of the IAM market include traditional hardware tokens, smart cards, and, increasingly, specifically designed software offerings for achieving secure, federated computing environments.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.