



The Security Division of EMC

White paper

Best Practices in Authentication: The First Step in the Path to Regulatory Compliance



“Developing, enforcing and auditing authentication and access control policies are a core element of compliance projects.” *

For the past ten years, governments and industry groups have enacted and published regulations in an effort to curb corporate financial malfeasance, identity theft and inappropriate access to personal data. Now, large and small companies around the world are grappling with mandates to comply with those regulations.

Compliance, while required and necessary, is not easy. Companies must often comply with multiple regulations, and do so in the context of other business objectives – such as 1) reducing costs, 2) improving customer service and employee productivity and 3) increasing revenue. Added to the challenge is that IT environments are constantly changing and new regulations are being added to the compliance mix. In this complex and dynamic environment, CIOs and IT departments are realizing

that a comprehensive approach to information security based on best practices is often the key to supporting regularity compliance initiatives on an on-going basis.

To help organizations in these efforts, RSA has developed an information security best practices framework. This framework can serve as a guide for companies looking to build flexible IT environments in support of regularity compliance. An essential component in this framework is a set of best practices in authentication. These best practices – when implemented – help an organization ensure that only authorized people are allowed access to corporate data, applications and systems.

*‘Trends 2005: Identity Management’,
Forrester Research, Inc., December 13, 2004

Contents

I. The Rise of Regulations	page 1
II. Who Must Comply?	page 2
III. Compliance Complications	page 2
IV. RSA Best Practices	page 2
V. Authentication: the First Step in Compliance	page 3
VI. Authentication Maturity Model	page 5
VII. RSA Authentication Solutions	page 5
Appendix 1 – Authentication Best Practices	page 7
Appendix II – Industries and Their Associated Regulations	page 8
About RSA	page 9

I. The Rise of Regulations

Corrupt corporate executives, identity thieves and hackers have certainly made their mark in the world. Pension plans and stock portfolios have been decimated, personal data stolen and used to empty bank accounts or otherwise perpetrate fraud, and once trusted systems violated and made vulnerable.

“LexisNexis, which compiles and sells personal and financial data on U.S. consumers, said Tuesday that personal information on 310,000 people nationwide may have been stolen.”

‘LexisNexis acknowledges more ID theft’,
CNN Money, June 2, 2005

“WorldCom overstated it’s results by more than \$5 billion over seven quarters, prosecutors said, though by other measures the fraud totaled \$11 billion.”

‘Bernie Ebbers Guilty’,
Forbes, March 15, 2005

This conduct – and the threat of it continuing – has shifted attention to the way systems are accessed: who is allowed into a system, how they are allowed to interact with data and how an organization knows the right people are getting in and the wrong people are staying out. Local and federal governments as well as industry groups around the world are rushing to require protection of systems, data and personal identities.

Some of the most publicized pieces of U.S. legislation include Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB) and the Health Insurance Portability and Accountability Act (HIPAA). These regulations mandate improved controls over financial systems or require protection of non-public personal information. At the state level, California’s SB 1386 and AB 1950 are examples of legislation that also protect personal information for customers, employees and prospects held by organizations. Outside the US, Japan’s

Personal Information Protection Act, Canada’s Personal Information Protection and Electronic Document Act, Australia’s Federal Privacy Act and the UK’s Data Protection Act are all mandating the protection of personal data in those geographies.

Meanwhile, industry groups are self-regulating in order to protect their customers and, ultimately, their members’ brands and revenues. One example is the Payment Card Industry (PCI) Data Security Standard created by a coalition including Visa, MasterCard, American Express and Discover and required for any member, merchant, or service provider that stores, processes, or transmits cardholder data.

The High Cost of Not Complying

Compliance with government regulations may seem onerous – time-consuming and expensive. But how expensive is failure to comply?

While regulations do specify fines and even jail time for failure to comply, the real cost to companies is in the loss of confidence and trust of customers, stock holders and employees. Financial scandals and numerous instances of identity theft – with some estimates of up to 5% of the US adult population being identity theft victims in 2004¹ – have caught the public’s attention. The names of companies such as ChoicePoint and CardSystems may forever be linked with mass identity theft.

It’s hard to put an exact price on this loss of trust. For companies such as CardSystems the loss of confidence may force it out of business.² Implementing a compliance framework based on information security best practices is one important way of showing key stakeholders that the organization is taking reasonable and appropriate steps to safeguard critical data, and as such is worthy of their continued business and on-going trust.

¹ Lawmakers say identity theft measure likely to pass this session, May 15, 2005, Newsday

² CardSystems says it faces ‘imminent extinction’, July 22, 2005, CNET News

II. Who Must Comply?

The array of regulations currently in place around the globe makes it nearly impossible to identify a headquarter location, sector, vertical industry, or company size that is immune from compliance. The examples below indicate some of the regulations faced by the companies described:

- A publicly-held, California-based restaurant chain may need to comply with SOX, PCI, SB 1386 and AB 1950.
- A publicly-held, UK headquartered, multi-national, pharmaceutical company that trades stock in the U.S. market must comply with SOX, 21 CFR Part 11, EU Annex 11, SB 1386 and AB 1950, EU Data Protection Directive, UK Companies Act and UK Data Protection Act.
- A Canada-based manufacturer selling goods throughout North America must comply with PIPEDA, SB 1386 and AB 1950.
- A privately-held Japanese company that sells goods via the internet to customers around the world must comply with the Japanese Personal Information Protection Law, SB 1386 and AB 1950, PIPEDA and EU Data Protection Act.
- A camera shop in New York City that also maintains an online store may need to comply with PCI, SB 1386 and AB 1950.

Even companies that are not singled out by a government regulation or industry standard often have to pay attention. Requirements to comply with a regulation often trickle down to business partners and suppliers who provide or use protected data. For example, a large HMO regulated by HIPAA might require an IT consultancy that interacts with customer records to meet standards for protecting that data.

Along with regulations, public awareness of financial and identity theft is beginning to redefine the standard of care by which businesses and service providers are judged. Evidence of this is a recent enforcement action by the Federal Trade Commission (FTC) against BJ Wholesale Club, Inc. for failure to take appropriate security measures to protect the personal information of thousands of customers. The FTC has found that the failure to take reasonable security measures was an unfair act or practice – even in the absence of a specific privacy or security policy or statement committing to take such measures.

III. Compliance Complications

The myriad of government and industry regulations are not prescriptive, only containing high level guidance on what organizations need to implement. Instead the government and industry bodies suggest or mandate using specific control frameworks for information on achieving regulatory compliance. For instance, SOX recommends adherence to COBIT; HIPAA and FISMA refer to NIST; GLB and Basel II to FFIEC; and AB 1950, EUDPD, 21 CFR Part 11, Annex 11 and the Japan Privacy Law to ISO 17799.³

Further complicating matters, as the earlier examples illustrate, is the need for many organizations to comply with several regulations and hence consider several control frameworks simultaneously. Lastly, organizations are faced with ever changing environments – both in terms of their own IT infrastructure as well as the overall regulatory environment. As a case in point, identity theft protection legislation that would mimic California's SB 1386 and AB 1950 is being considered in several states and at the federal level.

IV. RSA Best Practices

Regardless of the regulation or control framework in question, they all share common fundamental requirements to verify identities; allowing only authorized parties access to information. In order to satisfy these requirements organizations must consider solutions in the areas of:

1. Risk Management,
2. Authentication,
3. Access Control,
4. Data Protection and
5. Logging and Reporting.

From an information security perspective, these are the elements embodied in identity and access management solutions.

To help organizations with their compliance efforts, RSA, a leading provider of identity and access management solutions, has developed an exclusive set of some 60 information security best practices for compliance. Based on regulations and control frameworks, and utilizing the guidance of industry analysts and the SANS Institute along with experience gained through working with thousands of customers, RSA's best practice framework provides a way of developing an effective information security program to support your compliance efforts. (For more information on how RSA developed this framework see the sidebar 'The Development of a Best Practice Framework'.)

"Enhancing your authentication processes (and enforcing them) is the first step in the identity and access management process."

'Use This Eight-Step Process for Identity and Access Management Audit and Compliance',
Gartner Inc., March 28, 2005

V. Authentication: the First Step in Compliance

Implementing an effective compliance program starts with establishing who is who in an online world. This requires the development of authentication mechanisms that go well beyond simple passwords in order to establish a trusted identity for individuals within an organization. RSA includes 17 authentication best practices in its framework. The following section highlights several of these best practices to illustrate how RSA recommends companies implement robust authentication. (For a complete listing of authentication best practices, please refer to Appendix I.)

Only after authentication policies have been set and communicated can an organization be sure that they will be uniformly and effectively implemented and maintained.

The Development of a Best Practice Framework

RSA's Best Practice Framework helps organizations implement reliable compliance solutions. The framework was derived by extracting the key identity and access management related controls from the COBIT, NIST 800-53, ISO 17799 and FFIEC control frameworks and standards. These controls were then brought up to date with insights from:

- The SANS Institute (the largest source for information security training and certification in the world)
- Industry analyst recommendations
- RSA's experience with over 18,000 customers around the world

As an example of how the framework was developed, consider the authentication best practice recommendation to implement secure single sign-on systems. This best practice was derived from the following sources:

1. ISO 17799, section 9.3.1
2. FFIEC, pages 25-26
3. Gartner, Inc. ('Best Practices for Managing Passwords', Dec., 2003 and 'Use This Eight Step Process for I&AM and Compliance', March, 2005),
4. Forrester Research, Inc. ('Security Comparison: SSO vs. Password Synchronizations', Sept., 2004),
5. Giga ('Market Trends: Enterprise SSO', Dec., 2003) and
6. SANS Institute publication "Secure Implementation of Enterprise Single Sign-On Product in an Organization", July, 2004.

Each of the best practices in the RSA Best Practices framework comes from a similar rigorous audit of the regulations, control frameworks and deep industry knowledge. Organizations can use this framework as a starting point to establish their own set of information security best practices. As with any control framework or standard, it is intended to be tailored to an individual organization and their particular environment, objectives and industry.

RSA Best Practice

Develop and document a comprehensive authentication policy which dictates the use of mechanisms to validate user identity per system and/or application. All authentication techniques used should be governed by policy (e.g., password policy, remote access policy, certificate policy).

At the very least, authorized end-users should authenticate through presentation of a strong password. Since passwords may become compromised or broken with time, careful password management is critical.

RSA Best Practice

Ensure that passwords are changed regularly; lost or stolen authenticators are promptly reported and cancelled; and invalid credentials do not allow access to the system to keep authentication mechanisms effective.

However, even strong passwords (those 8 characters in length and combine numbers, letters and symbols) that routinely change present vulnerabilities. Furthermore the definition of what is a strong password today may change as computing power continues to increase.

RSA Best Practice

Use multi-factor authentication when a strong password policy causes users to take actions which weaken security such as writing passwords down; or causes users to constantly forget passwords, which jeopardizes the timely availability of information for authorized users. Consider adding a multi-factor authentication mechanism for remote or Internet access, for use by system administrators, to protect critical systems and for legacy systems and applications that can not accommodate strong passwords.

“Increasing password length and complexity can yield an increase in security, but it places additional burden on users. The breaking point is near, if not already reached. For stronger authentication, consider using stronger authentication methods, rather than increasing the length and complexity of passwords.”

‘Passwords are near the breaking point’,
Gartner Inc., Dec 6, 2004

Since human beings are involved in password and multifactor authentication processes, it can always be assumed that emergencies will occur, sometimes frequently. Lost and/or stolen passwords and other authenticators are more than an annoyance. They keep people from important data which slows productivity and hampers business.

RSA Best Practice

Set up emergency access procedures to provide timely access to resources when users forget their passwords or are not in possession of their authenticators, using a technique which can confirm the user’s identity with a high level of assurance. Automated mechanisms should be used to facilitate emergency access.

Along with implementing password or multi-factor authentication policies, companies must tighten logon procedures.

RSA Best Practice

Implement single sign-on (SSO) systems where feasible so users do not have to remember or possess multiple authentication mechanisms, providing for the use of stronger passwords or other authentication methods and fewer user-created weaknesses.

Single sign-on systems effectively reduce the number of passwords a user requires to access corporate applications and systems. There are fewer passwords to remember, fewer to lose, fewer to be stolen. There are fewer calls to the help, less work for IT administrators.

To further improve and secure logon procedures, single sign-on and two-factor authentication should be combined.

RSA Best Practice

Use multi-factor authentication or ensure the use of strong passwords for single sign-on (SSO) environments which provide access to multiple applications or systems containing confidential or critical data. For SSO, where feasible, multi-factor authentication is recommended.

Together, two-factor authentication and single sign-on give end-users one, easy way to logon to all the systems they must access and the IT department one, easy, reliable, repeatable authentication practice to administer.

VI. Authentication Maturity Model

Implementing best practices may seem daunting at first, but is very possible if done in stages, much like you'd take a long road trip. The first step in planning any leg of a trip is pinpointing your starting place and gauging the resources available to get to the next stop.

You can similarly plan a step-by-step implementation path for the best practices most critical to your organization. What do your authentication policies and procedures look like today? How much time and budget will you spend on improvements? When do your compliance deadlines hit? When is your next audit? This "trip" should be planned in the context of your overall Information Security requirements and, more specifically, your overall authentication maturity.

Multi-factor authentication

In multi-factor authentication, a user must present something they have (e.g. access card, hardware token) as well as something they know (e.g. a secret PIN or password). Using an ATM card is a familiar example of multi-factor authentication, where the banking customer must provide both the card and a memorized PIN to access accounts and complete transactions. Multi-factor authentication systems provide the user with the same simplicity and ease of use of passwords but are much more secure.

VII. RSA Authentication Solutions

RSA solutions are designed to fit seamlessly into the existing e-business infrastructures, easing the implementation and maintenance of compliance programs. In use by over 18,000 companies around the world, they are developed with best practices in mind.

RSA SecurID® Solutions. RSA SecurID technology delivers strong, two-factor authentication. Users access systems after providing a password or PIN (something they know) and a second authentication code that's provided by either software or a device (something they have). This provides a much more reliable level of user authentication than reusable passwords.

Through integration with hundreds of leading products, RSA provides a wide range of user authentication options that help positively identify users before they interact with mission-critical data and applications.

RSA SecurID for Microsoft® Windows®. By replacing vulnerable passwords with two-factor authentication, RSA makes it possible to positively identify users before granting them access to valuable corporate resources accessed through Windows desktops and networks – while simultaneously delivering a simplified and consistent user logon experience.

RSA® Digital Certificate Management Solutions. RSA provides a family of interoperable modules for managing digital certificates and creating an environment for authenticated, private and legally-binding electronic communications and transactions. Digital certificates provide a solid technical infrastructure to secure data throughout an organization and to meet a wide-range of regulatory requirements. Certificate-based applications enabled by RSA's digital certificate solutions include:

- Strong authentication,
- Digital signatures,
- Web server security,
- Secure e-mail and
- Secure VPNs.

Starting place	Your authentication practices look like:	Move ahead with
At risk	<ul style="list-style-type: none"> - Inconsistent password practices across applications - Shared username/passwords - No password strength or time-out controls 	<ul style="list-style-type: none"> - Creating consistent password specifications, including standards for strength and duration of passwords - Assigning usernames and password for each individual and application
Basic	<ul style="list-style-type: none"> - Minimal password policies are in place - User identities are controlled within individual applications - Users authenticate to individual applications exclusively with passwords 	<ul style="list-style-type: none"> - Implementing multi-factor authentication for remote access and for system administrators - Putting strong password policies in place - Deploying single sign-on systems to ease the user burden of remembering complex passwords
Common Practice	<ul style="list-style-type: none"> - Multi-factor authentication in place for remote users and system administrators - Strong password policies coupled with single sign-on systems utilized throughout the organization 	<ul style="list-style-type: none"> - Implementing multi-factor authentication for access to sensitive applications and/or to single sign-on systems
Best Practice	<ul style="list-style-type: none"> - Strong password policies and management systems in place for all application environments - Multi-factor authentication in place for remote users, system administrators and single sign-on environments 	<ul style="list-style-type: none"> - Passing application assertions across enterprise or organizational domain boundaries

Additional Information

For additional information about using our interactive Authentication Scorecard spreadsheet to evaluate your authentication options, contact your RSA sales representative or channel partner or visit www.rsa.com and click on "contact".

Appendix 1 – Authentication Best Practices

Policy & Process

1. Develop a comprehensive authentication policy
2. Implement appropriate authentication techniques
3. Keep authentication mechanisms effective
4. Protect storage & transmission of authentication information
5. Control authentication for access to external systems
6. Maintain business continuity for authentication services.

Authentication Methods

7. Develop & enforce a strong password policy
8. Protect against social engineering attacks
9. Use multi-factor authentication when strong passwords fail
10. Use multi-factor authentication for remote access
11. Use robust authentication techniques for single sign-on
12. Use multi-factor authentication for system administrators

Logon Procedures

13. Implement secure single sign-on systems
14. Control display of information in the logon procedure
15. Terminate logon procedure after unsuccessful attempts
16. Implement time-out procedures after inactivity
17. Set up emergency access procedures

Appendix II – Industries and Their Associated Regulations

INDUSTRY	REGULATION
U.S. healthcare organizations	Health Insurance Portability & Accountability Act (HIPAA)
Companies traded on a public exchange in the U.S.	Sarbanes-Oxley (SOX)
U.S. financial institutions	Gramm-Leach-Bliley (GLB)
FDA regulated companies	21 CFR Part 11
Global financial services organizations	Basel II
Processors of personal data in the European Union	EU Data Protection Directive (DPD)
Private companies in Japan which handle personal information	Japanese Personal Information Protection Law
All Organizations in Canada	Personal Information Protection & Electronic Documents Act (PIPEDA)
Organizations with customers in California	California SB 1386 and AB 1950
Producers of medicinal products sold in the EU	EU Annex 11
U.S. Federal Government agencies	Federal Information Security Management Act (FISMA)
Entities that store, process or transmit card holder data	Payment Card Industry (PCI) Data Security Standard
UK companies audited by the Financial Reporting Review Panel	UK Companies Act
U.S. healthcare organizations	Health Insurance Portability & Accountability Act (HIPAA)

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2006-2007 RSA Security Inc. All rights reserved.

ASC WP 0607



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC