



The Role of Password Management in Achieving Compliance

White Paper

PistolStar, Inc.
PO Box 1226
Amherst, NH 03031
USA

Phone: 603.546.2300
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

The Role of Password Management in Achieving Compliance

Overview

Password management solutions have had a dramatic impact on organizations; from eliminating password-related Help Desk calls to simplifying end-user access, password management has gone beyond tightening security to delivering improvements to the bottom line. Now, with the implementation of Sarbanes-Oxley, HIPAA and other regulations, password management has proven to be a strategic component for successful compliance.

Table of Contents

Introduction	1.0
Regulatory Compliance Entails Securing Critical Data	1.1
Purpose and Overview	1.2
Password Management: More Than Security	2.0
The Beauty of Password Management	2.1
What Governmental Regulations Require	2.2
What Password Management Systems Should Provide	2.3
Password Management Solutions Facilitating Compliance	3.0
PistolStar's Password Power and Web Set Password	3.1
Meeting the Challenges of Compliance	3.2
Increasing Security and Reaping Bottom Line Results	3.3
Summary	4.0
Appendix A – System Requirements	5.0
Appendix B – Resources	6.0

*The Role of Password
Management in Achieving
Compliance*

1.0 Introduction

1.1 Regulatory Compliance Entails Securing Critical Data

Compliance with governmental regulations has not only been a hot issue for corporate management, but a major concern of IT departments as well. These regulations mandate that organizations protect and secure access to sensitive financial data and customer and patient information, dramatically impacting the IT infrastructure as well as business processes.

In the past decade, several laws have passed that have forced organizations to establish corporate compliance policies. The three most significant laws are:

Sarbanes-Oxley Act (SOX) – A reaction to the accounting scandals occurring in 2001 and 2002, SOX requires publicly-traded companies to implement controls with respect to specific internal business processes. This necessitates having an outside auditor certify the accuracy of financial statements and performing an annual assessment of internal controls relating to the security of critical data, particularly financial information.

Health Insurance Portability and Accountability Act (HIPAA) – Requires that health institutions employ procedures that protect the disclosure of an individual's personal health information, ensuring the privacy and security of that information as it is collected, processed and transferred to other health organizations.

Gramm-Leach-Bliley Act (GLB) – Requires that financial institutions (and persons that receive protected information from financial institutions) adopt strict measures for protecting the privacy and security of customer data.

Because of these laws and others, such as SEC Rule 17a-3/17a-4 and the Electronic Signatures Act, organizations have been compelled to implement strategies for retaining critical data and assuring corporate governance. Consequently, to maintain the security of databases and their intranet, an organization's IT department is challenged with the task of ensuring there is a compliance architecture in place.

Several types of technologies should be considered to support compliance. They include:

- Data storage and backup/recovery systems to maintain historical data and provide on-demand access;
 - A high-speed LAN infrastructure to support collaboration and provide real-time information for viewing what's occurring in the organization at any given moment;
 - Broadband WANs and extranets to conduct operations around the globe and facilitate collaboration with partners and governance entities;
 - Centralized compliance process and risk-management software to be integrated with existing and planned business applications; and, most importantly,
 - Security systems, such as authentication, encryption and end-user passwords, to safeguard against unauthorized access and/or fraud and data theft.
1. Passwords are the right of entry to the servers, applications and intranets on which critical data is stored, and they are essential for securing these areas from unauthorized persons.

Compliance with governmental regulations has not only been a hot issue for corporate management, but a major concern of IT departments as well.

2. Accordingly, password management can play a key role in protecting data and files that are the focus of corporate compliance.

As organizations coordinate their response to the recent governmental regulations and begin implementing the necessary changes, there are many IT solutions that should be considered. However, password management is the most instrumental in controlling and securing access to protected information and it should be a significant part of any organizations' compliance strategy.

1.2 Purpose and Overview

While password management offers organizations peace of mind as a result of enhanced system security and improvements in end-user and Help Desk productivity, specific capabilities also contribute significantly to achieving compliance.

This paper will look at the dramatic impact password management solutions have had on organizations. From eliminating password-related Help Desk calls to simplifying end-user access, password management has gone beyond tightening security to delivering improvements to the bottom line. Now, with the implementation of Sarbanes-Oxley, HIPAA and other regulations, password management has proven to be a strategic component for successful compliance.

We will explore the numerous ways in which password management capabilities aid in compliance, addressing the requirements of the three main governmental regulations: Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley. We'll then identify the specific password management capabilities that support compliance, delving into what organizations should look for when investigating password management solutions.

In closing, we'll present two software solutions that provide the secure password management capabilities that organizations need and will help satisfy the access control and data protection requirements of governmental regulations.

From eliminating password related Help Desk calls to simplifying end-user access, password management has gone beyond tightening security to delivering improvements to the bottom line.

2.0 Password Management: More Than Security

2.1 The Beauty of Password Management

Passwords are vital to gaining access to servers, applications, the Web, intranets, and extranets across and beyond the enterprise. Organizations can secure specific areas of their networks by utilizing passwords to prevent access from unauthorized persons.

The introduction of password management solutions has allowed organizations to increase and maintain corporate security, protecting important applications, data, and files. Most importantly, password management has helped IT departments address two of their biggest challenges:

Securing the password authentication process without increasing calls to the Help Desk about resets; and heading off network intruders who attempt to gain access to critical data and files by guessing passwords or seizing upon weak ones.

Password management solutions primarily evolved from the many issues created because of the widespread corporate use of passwords, particularly the

necessity of having multiple passwords for accessing the numerous servers, directories and applications in an enterprise. Having to remember numerous sets of credentials and which password to use for each application creates frustration for end-users and increased calls to the Help Desk because of lost or forgotten passwords and the need to create new ones. IT experiences huge overhead, while both administrators and end-users suffer lost productivity due to the time required for creating new passwords manually.

To restore overall productivity and also respond to the increasing number of corporate employees who are working remotely and at non-traditional hours, one of the most welcome capabilities of password management is self-service password management, which allows end-users to create and reset their own passwords, without contacting IT for assistance.

With multiple passwords, synchronization can also be problematic since password policies are frequently disparate. Most often, it is the password quality and password expiration settings that are dissimilar for various passwords. Password management automatically enables accurate synchronization of passwords, ensuring uninterrupted access.

Security also becomes an indisputable concern with multiple passwords in use, because end-users often leave passwords jotted on notes left on or near their computers. To address all the issues arising from assigning end-users with numerous usernames and passwords, companies are deploying solutions that will simplify and secure the password authentication and management process for end-users, thereby freeing up the time and resources used by IT to respond to password-related calls. An added and critical benefit of password management is its numerous capabilities that also aid in achieving corporate compliance.

An added and critical benefit of password management is its numerous capabilities that also aid in achieving corporate compliance.

2.2 What Governmental Regulations Require

There is a significant overlap in the requirements raised by the main corporate governance and privacy regulations, as outlined below. Common requirements that are satisfied by password management capabilities are:

1. Strong and reliable authentication
2. Strict control over end-user access to systems and data, including timely removal of access after an employee departure
3. Thorough audit trails and reporting on end-user access to specific systems and data

The following summarizes the password security and management requirements of each regulation.

Sarbanes-Oxley (SOX) – There are several components to SOX, but it clearly stipulates that organizations are required to establish an “adequate internal control structure,” including control over system access. Sections 302 and 404 of SOX specifically require CEOs and CFOs to ensure their business processes are under control.

Password management solutions facilitate SOX compliance by:

- Ensuring end-user access to only those systems and applications required for their jobs;
- Enforcing strong password policies, especially for end-users who have access to sensitive or protected records;
- Ensuring enterprise access privileges are removed when an employee

- leaves the organization;
- Eliminating end-users' need to share authentication information with the Help Desk or IT staff for password reset or system access;
- Automating password reset processes to eliminate human error; and
- Ensuring complete, accurate audit trails for all changes in access rights.

HIPAA – For healthcare organizations such as hospitals, physicians' group practices, insurance carriers, and HMOs, HIPAA presents major challenges to maintain the privacy of an individual patient's personal health information. To ensure compliance, these organizations not only need to train employees on privacy measures and have someone appointed to oversee privacy initiatives; more importantly, they need to secure access to patient records.

Password management solutions meet the challenges of HIPAA compliance by:

- Enabling strict authentication and enforcing strong password policies for end-users with access to patient records;
- Protecting disclosure of a patient's personal health information by ensuring that access to patient's records is only granted to authorized end-users and is immediately rescinded when an authorized end-user leaves the health care organization;
- Implementing automated and self-service processes for creating and managing passwords; and
- Tracking login attempts and reporting on access to protected areas to capture any suspicious or unauthorized activity as well as changes in access rights.

Password management solutions meet the challenges of HIPAA compliance by protecting disclosure of a patient's personal health information by ensuring that access to patient's records is only granted to authorized end-users and is immediately rescinded when an authorized end-user leaves the health care organization..

Gramm-Leach-Bliley (GLB) – The GLB Act is directed at all financial institutions, including banks, securities firms and insurance companies, and requires the adoption of strict measures for protecting the privacy and maintaining the security of customer information. The guidelines stipulate that these organizations must control risks to customer information, protect against threats to the security and integrity of customer records, guard against unauthorized access to these records, and implement authentication processes that only allow access to authorized employees.

Password management solutions contribute to GLB compliance by:

- Enforcing password policies for end-users with access to customer information;
- Ensuring access to customer records is disabled as soon as employees leave financial institutions;
- Eliminating end-users' need to share authentication information with the Help Desk or IT staff for password reset or system access;
- Automating password reset processes; and
- Ensuring complete, accurate audit trails for all changes in access rights.

2.3 What Password Management Systems Should Provide

Clearly, to satisfy the authentication and access management needs of corporate compliance, organizations should ensure their password management system offers the following capabilities:

- Secure password authentication processes;
- Strong password quality;

- Enforced security and password policies to ensure passwords are not only strong (and not easily guessable), but also changed on a regular basis;
- Unified password policies for ensuring accurate password synchronization;
- Secure and controlled access by end-users;
- Secure and automatic password creation and reset processes;
- Self-service capabilities that allow end-users to manage their own account and perform their own password resets and recovery, ensuring they have complete understanding of the systems and data to which they have access; and
- Reporting on login attempts and end-user requested access to specific data.

Password management is one of the most beneficial technologies for achieving compliance. When deployed, password management not only reduces costs and increases security, but makes compliance with governmental regulations easier and more demonstrable.

3.0 Password Management Solutions Facilitating Compliance

When deployed, password management not only reduces costs and increases security, but makes compliance with governmental regulations easier and more demonstrable.

3.1 PistolStar's Password Power Web Set Password Plug-In

With a focus on continually simplifying access and further easing password management woes for end-users, PistolStar has delivered Password Power 8, its password management solution. With this product, PistolStar has responded to its customers' compliance needs by ensuring robust password authentication, controlled system access, and consistent enforcement of corporate security policies.

Password Power 8

Password Power 8 encompasses password plug-ins for IBM System i, Oracle, SAP, LDAP, Microsoft Active Directory and Windows, Novell eDirectory and IBM Lotus Notes ID, Domino HTTP, and Sametime. Password Power simplifies the password authentication process for any end-user maintaining separate passwords for these applications by allowing them to enter only their password for Windows, Microsoft Active Directory, Sun ONE LDAP, or Novell eDirectory to gain access. Password Power also enables self-service password resets, including Windows password reset and use of the Windows password to recover the Notes ID.

Combining the functionality of multi-password synchronization with single sign-on, Password Power reduces the number of times an end-user must supply log-on information during a Windows session to a single instance. As a result, end-users only need to remember and make changes to one password in one place. When a new password is implemented in Windows, the Internet passwords and, optionally, the Notes ID file password, are automatically updated.

Password Power also helps to maintain and enhance the security of corporate data. During the syncing process, the password security policies (e.g., password expiration and password quality) implemented by the administrator through Windows are automatically transferred to the other passwords, ensuring the coordination of disparate password policies.

Web Set Password Plug-In

With our Web Set Password Plug-In, companies can increase password security and provide self-service functionality to end-users. Password Power's Web Set Password Plug-In offers over 36 password authentication features not available in Lotus Domino R6 and 7, including single sign-on, browser-based password synchronization and self-service password reset, enabling end-users to access Lotus applications from the Lotus Notes client by authenticating with their network logon —either their Windows or directory password (Microsoft Active Directory, Novell eDirectory, and Sun ONE LDAP).

3.2 Meeting the Challenges of Compliance

These password management solutions support the system access management and data protection requirements of SOX, HIPAA, and GLB. The following are their compliance-related capabilities:

- Facilitating and enforcing the use of stronger passwords;
- Ensuring employees only have access to systems and information required for their jobs;
- Guaranteeing accounts are disabled and access is completely revoked when employees leave company;
- Automating password reset processes to eliminate human error;
- Ensuring complete, accurate audit trails and reports on all account changes, login attempts;
- Enforcing password policies that require passwords to be strong and changed regularly;
- Confirming unified password policies via accurate password synchronization
- Enabling strong authentication; and
- Protecting sensitive corporate and customer data through encryption.

In addition to aiding compliance, Password Power and its Web Set Password Plug-In, provide tremendous cost-savings by decreasing Help Desk calls and heading off potential security breaches caused by issues that can arise in the password authentication and management process.

3.3 Increasing Security and Reaping Bottom Line Results

Companies implementing Password Power can realize a significant and immediate return on investment (ROI). In addition to aiding compliance, these solutions provide tremendous cost-savings by decreasing Help Desk calls, which can drain support staff time and money, and heading off potential security breaches caused by issues that can arise in the password authentication and management process.

Both IT administrators and end-users benefit in several ways. Administrators can address specific problems and challenges, such as enabling secure access to corporate intranets and extranets, and protecting applications and content from illegal usage. They can also achieve security “best practices” through the ability to define password rules and numerous password preferences related to password quality, history, expiration, 3-strikes and last login.

End-users only need to remember and change one password instead of several, eliminating the frustration that results from the difficulty of remembering multiple passwords and greatly decreasing the likelihood passwords will be written down and become a target for internal network intruders.

End-users also have the convenience of performing password resets via self-service functionality that allows them to securely manage and reset their passwords directly from a Web browser, and without Help Desk intervention. By removing the need to engage IT and wait for a new password to be created, Password Power and its plug-ins reduce end-users' downtime and allow both administrators and end-users to be more productive.

Password management has already earned respect as a valuable solution by meeting corporate objectives such as diminishing employee downtime, increasing end-user and IT productivity, and incorporating security “best practices.” By also playing a significant role in achieving compliance, password management can have a profound impact on an organization’s bottom line, drawing the attention of senior management and reigning at the top of the “must-have technologies” list.

4.0 Summary

Complying with recently established governmental regulations is currently paramount in the minds of organizations. To be compliant, organizations need to ensure they are protecting critical financial data and reports, and patient and customer information, requiring they formulate a strategy to create compliance policies and build a compliance infrastructure. Several departments are impacted, but none more so than IT, which is responsible for the security of the organization’s networks and the information and files contained with them.

Several technologies should be considered when mounting a compliance strategy, including an IT security system that features password authentication and management. While the financial investment of implementing technology for compliance purposes can be cost-prohibitive, password management is an inexpensive solution that is efficient, delivers benefits in several areas, and demonstrates a return on investment.

Password management systems are available that address several needs, such as password security, authentication, access management, and self-service functionality. Organizations that need to comply with one or more governmental regulation should ensure their password management system delivers strong passwords, provides secure authentication, and enforces security and password policies through “best practices.”

Organizations that are required to achieve compliance need to act quickly, as they risk legal action as well as stiff government fines and restrictions. With the time and financial commitment involved with strategic planning, creating compliance policies and investing in technologies, it is reassuring that there is one solution that will efficiently and cost-effectively meet their needs. With password management, organizations can meet the challenges of compliance.

5.0 Appendix A

System Requirements

Password Power 8

Password Power is a client-side solution with an optional server component that integrates seamlessly and does not require end-user setup. Password Power’s server-side capabilities support Windows, Linux, Solaris, and IBM AIX 5.1. On the client side, Password Power supports Microsoft Windows NT, 2000, and XP.

With the time and financial commitment involved with strategic planning, creating compliance policies and investing in technologies, it is reassuring that there is one solution that will effectively meet their needs. With password management, organizations can meet the challenges of compliance.

Web Set Password Plug-In

Password Power's Web Set Password Plug-In (WSP) is a server-side solution that integrates seamlessly with IBM Lotus technology and does not require end-user setup. WSP supports System i, IBM AIX 5.1 and higher, Linux, Sun Solaris UltraSPARC, and Microsoft Windows Server 2003 and Windows NT, 2000, and XP.

6.0 Appendix B

Resources

"The Myths & Realities of Domino 6 Password Management," PistolStar White Paper, July 2004.

http://www.pistolstar.com/forms/responseforms/MRD_IP_LP.html

"The Evolution of Password Authentication and Management: Simplifying It Without Having a Complicated Solution," PistolStar White Paper, January 2005.

http://www.pistolstar.com/forms/responseforms/EPAM_IP_LP.html

*PistolStar serves
Global 2000 companies
and organizations
across multiple vertical
industries including
automotive, chemicals,
consumer products,
finance/banking, gov-
ernment, healthcare,
manufacturing, adver-
tising and media, com-
munications, pharma-
ceuticals and retail.*

###