



# Compliance and Beyond

*Toward a Consensus on  
Identity Management Best Practices*

## TABLE OF CONTENTS

---

<b>Introduction .....</b>	<b>2</b>
<b>The Impact of the Global Regulatory Wave.....</b>	<b>2</b>
<b>Best Practices in Risk Assessment and Security Policy Setting .....</b>	<b>4</b>
<b>Best Practices in Security Policy Enforcement .....</b>	<b>6</b>
<b>Best Practices in Monitoring and Reporting .....</b>	<b>7</b>
<b>Beyond Compliance .....</b>	<b>8</b>
<b>OneSign: Exemplifying Best Practices in Identity Management.....</b>	<b>10</b>
<b>Appendix: The OneSign Product Family .....</b>	<b>10</b>

## INTRODUCTION

When the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996, for more than a decade, government and industry bodies around the world have issued a growing number of regulations designed -- in whole or in part -- to ensure the security, integrity and confidentiality of personal and corporate data. These mandates span a range of industries, from financial institutions to healthcare providers to utilities firms to retailers and beyond. Regulations are often mandatory and compliance must be verifiable. In many cases, organizations and their company officers found to be non-compliant may be subject to fines or legal action, in addition to facing exposure to risks associated with internal data breaches.

The specific details of these regulations are as varied as the industries they serve. However, most contain sections that require companies to secure each user's credentials and manage all access to IT-based systems. Taken together, these individual regulatory guidelines point toward a growing consensus of what constitutes best practices in identity management and IT security.

At the same time, as organizations have undertaken programs to ensure compliance with these regulations, a similar consensus has begun to emerge on how to achieve compliance. Forward-thinking companies are now exploring how to do this affordably while ensuring maximum user convenience and satisfaction. This white paper explores these compliance-driven best practices, how OneSign solutions support them, and how prioritizing their implementation makes good business sense beyond the fulfillment of compliance requirements.

## THE IMPACT OF THE GLOBAL REGULATORY WAVE

Terrorist sabotage. Identity theft. Credit card fraud. Corporate malfeasance. Privacy violations. Many critical problems facing society today involve unauthorized access to, and use of personal and other confidential data. So it is no wonder that government agencies and industry organizations continue to issue guidelines and regulations that, to one degree or another, safeguard confidential data and access to it.

These guidelines and regulations span a growing number of industries, affect organizations of all sizes, and often cross international borders. Moreover, they often require companies to invest significant amounts of time, capital, and human resources to achieve and maintain compliance. Among the most well-known guidelines and regulations are the following:

### *Basel II.*

The Basel Committee on Banking Supervision, a global industry regulatory body, published the Basel II standard in 2004 with the goal of ensuring that banks have sufficient capital set aside to guard against financial and operational risks. Basel II also requires banks to examine IT, security, fraud, employment practices and workplace safety, business services, physical damage, business disruption, system failure, service execution-delivery-process management, and legal and reputation factors.

### *Federal Financial Institutions Examination Council (FFIEC) standards.*

In August of 2001, the FFIEC first issued a set of comprehensive requirements for securing authentication in an "electronic" banking environment. Growing adoption of consumer-based electronic banking led the FFIEC to deliver a second guidance note in August of 2005, this time focusing on authentication in an "internet" banking environment. These regulations require encryption in all online transaction processing (OLTP) done by financial institutions, and are designed to prevent unauthorized disclosure of personal data, whether involving external transactions with consumers or internal transactions related to consumers. The FFIEC standards require ongoing risk assessments to ensure compliance.

***Food & Drug Administration (FDA) Title 21 Code of Federal Regulations (CFR) Part 11.***

This regulation requires pharmaceutical companies, medical device manufacturers, and other FDA-regulated industries to implement controls, including audits, validation systems, audit trails, electronic signatures, and documentation for software and systems involved in processing many forms of data as part of business operations and product development.

***Gramm-Leach-Bliley Act (GLBA).***

Passed by the U.S. Congress in 1999, GLBA's primary purpose was to modernize the financial services industry by allowing greater competition among banks, securities companies, and insurance firms. However, a key component of the legislation set new requirements governing the collection, disclosure, and protection of consumers' nonpublic personal information, or personally-identifiable information.

***Health Insurance Portability and Accountability Act of 1996 (HIPAA).***

Among its many provisions, HIPAA established formal regulations designed to require healthcare providers to protect the confidentiality and security of patient information. In addition to mandating new policies and procedures, the HIPAA security regulations require mechanisms for controlling access to patient data on healthcare providers' information technology (IT) systems.

***North American Electric Reliability Corporation (NERC) / Critical Infrastructure Protection (CIP).***

In response to increased government oversight, the utilities industry, through NERC, issued new cybersecurity regulations in 2006 regarding the protection of critical infrastructure, including both physical and IT assets, at utilities companies. These regulations will be enforced through periodic auditing with the prospect of fines for non-compliance starting in mid-2010.

***Payment Card Industry (PCI) Security Standard.***

Amid mounting concerns about identity theft and credit card fraud, leading companies in the payment card industry established the PCI Security Standard, which is designed to enhance payment account security among merchants, financial institutions, payment processors, and point-of-sale providers. Ultimately, the more than one billion global payment card users will benefit from stronger security at all points of the transaction process, lessening the chance of individual data theft.

***Sarbanes-Oxley Act (SOX).***

Created in the wake of major corporate governance scandals, this 2002 law mandated comprehensive control structures and procedures regarding financial data at publicly-held companies.

This is only a small selection from a much larger list. Similar laws, statutes, and standards can be found throughout the world, including: FIPS 201, FIPS 140-2, Patriot Act, FISMA, California Assembly Bill 1950, California Information Practice Act Senate Bill 1386, PIPEDA-Canada, EU Data Protection Directive, Turnbull Guidance 1999-UK, The Companies Act 1985 Regulations-UK, The Companies Act 2004-UK, Money Laundering Regulations-UK, UK Data Protection Act, Freedom of Information Act-UK, EU Privacy and Electronic Communications Regulations 2003-EU, EU Annex 11, Japan Personal Information Protection Act 2003, Federal Privacy Act 1988-Australia, NEN7510-Netherlands... and many more.

Recently, Imprivata conducted an analysis of these major guidelines and regulations. The result of this analysis is a set of common IT security recommendations that can apply to multiple industries. By mapping these regulations and requirements against the capabilities provided by Imprivata OneSign solutions, this white paper has assembled what could be considered a recommendation for best practices in identity management, according to a consensus of leading government and industry regulatory bodies.

## **BEST PRACTICES IN RISK ASSESSMENT AND SECURITY POLICY SETTING**

### ***Create and maintain appropriate policies, procedures, and controls that define a company's approach to authentication and access.***

OneSign safeguards information by enabling secure and compliant access to networks through local or remote access and SSO enabled applications.

Through a non-intrusive and easy to use appliance, OneSign allows administrators to create and manage a wide range of authentication policies for users, groups and computers that can take into account access means (offline, local or remote), user location, and badge status.

With OneSign, users cannot access the network or an application unless they have the proper authorization credentials, based on the user's identity, role within the organization, and location. Credentials can be username + strong password, One-Time Password tokens, biometrics, proximity-based cards (passive and active), contact smartcards, or national ID cards. These authentication mechanisms can be tailored to meet the security needs of the customer, and extended to two- or three-factor if desired.

### ***Map policies to users, computers, locations and specific business processes or application content.***

OneSign provides the ability to link a user, computer, or location into a policy that can control offline, local, or remote access based on company policy or the end users' needs or requirements.

### ***Manage user identity, authentication, and access to systems.***

OneSign administrators can specify a flexible access policy that controls the users' ability to access applications through local or remote networks. The OneSign admin can specify constraints in the policy, including:

- Allowing local, remote or offline access to specific users or groups;
- Requiring strong passwords or other forms of strong authentication;
- Locking out users after a pre-determined number of failed login attempts;
- Enforcing a specified lock-out time period before allowing users to reattempt network or application login;
- Allowing self-service password reset after proper identification questions are answered;
- Logging off users after a specified period of inactivity, set by the administrator;
- Disabling offline logon after a specified number of days, based on the organization's predetermined best practice policy;
- Removing inactive users after a specified number of days according to company policy;
- Implementing the use of randomly-generated passwords, unknown to the user, for logging into applications at regular password reset intervals;
- Specifying the physical locations where the logon request can occur. This constraint can be specified down to the specific set of doors that secure the work area.
- Creating accounts within the OneSign Domain to support authentication of temporary workers that don't have network logons.
- Defining authentication using the embedded Radius server to allow OneSign users to logon through a VPN or SSL VPN gateway.
- Managing the issuance of Vasco tokens to users to One Time Password authentication for network, remote and offline logons.

When a person's employment at a company ends, OneSign can immediately lock the user's ability to log onto OneSign-protected networks and applications. This can be done: manually, by the OneSign administrator, automatically, via integration with a User Provisioning System; or automatically using OneSign Physical/Logical, when the Physical Security staff disables the employee's badge.

***Ensure data confidentiality and integrity to reduce identity theft.***

OneSign manages passwords for each OneSign-enabled application system. Default passwords can be disabled or changed on production systems before putting a system into production to close down the obvious system logons. OneSign also provides mechanisms to positively identify each user via a range of authentication options that help to reduce the risk associated with theft or compromise of trusted user identity information through inadequate logon security. As a secure store for all the log-on credentials associated with the enterprise, OneSign eliminates the use of "sticky notes" with written-down passwords that can compromise the security of the entire system. OneSign utilizes secure, encrypted communications between administrators or users and the OneSign server. All log-in data is securely communicated to the OneSign server using AES-128 bit encryption and Imprivata's patent-pending secure transmission technology.

***Measure user acceptance, performance, scalability, and system interoperability.***

OneSign is designed to ensure reliable performance even with large numbers of users. OneSign is packaged as a self-contained, purpose-built appliance that supports business continuity requirements through full database replication over distributed applications. A single OneSign appliance can support up to 50,000 users. An unlimited number of users can be supported with the OneSign web services architecture that allows either clustering of appliances within a data center or distributed appliances spread over multiple sites. Replication of the critical meta data across multiple appliances is done using Oracle streams a prove mission critical component that has demonstrated scalability and reliability.

User convenience is a key OneSign strength. It has been acclaimed within the industry for its ease-of-use, rapid SSO-enabling of applications and non-invasive approach to directories and applications. OneSign is rated highly because it is virtually transparent to end-users and requires no changes in behavior that could disrupt work or limit productivity. OneSign is also designed for maximum interoperability with complementary identity and access management solutions. It integrates easily with all leading Directory Servers and User Provisioning systems. It supports a broad range of strong authentication devices -- a number of these without requiring a standalone server. Fingerprint identification, for example, is supported directly from the OneSign Server. OneSign also integrates with leading Physical Access Control Systems (PACS) and, through RADIUS, can authenticate users to IPsec or SSL VPN gateway servers.

***Coordinate risk assessments with central risk management authorities.***

OneSign's advanced auditing capability provides a single point of correlation for all activities surrounding user log-on for offline, network, remote, and application access. With OneSign, a comprehensive, identity-based timeline is maintained to support forensic investigations and compliance reporting. An important feature is the ability, especially with OneSign Physical/Logical, to build a timeline that includes physical location down to the last door opened before logging onto the computer. This has value not only for forensic investigations, but also as a deterrent by being able to create stronger linkages between the application log-on and the identity of the user.

## **BEST PRACTICES IN SECURITY POLICY ENFORCEMENT**

*Provide enterprise-wide control over authentication tools that are integrated with the organization's IT security framework.*

OneSign monitors authentication activities for both local and remote access and can generate real-time notifications for different conditions either as http posts or emails to administrators. This vendor-neutral approach allows OneSign to generate an alert, for example, if an account has failed to successfully log-in after a number of tries. This notification might indicate an account hacking activity or a user who has forgotten his/her password. OneSign can also be used to publish audit logs in standard SYSLOG format for output to any enterprise-level Security Information Event Management (SEIM) tool.

*Prevent unauthorized access to resources; manage user account lifecycle; manage review of accounts; manage and monitor third-party access and interfaces.*

OneSign can prevent unauthorized access by automating password changes and hiding these credentials from the end-user, thereby removing the ability to access a OneSign-enabled environment from the outside. These passwords can be set at the maximum complexity supported by the application to ensure an even greater level of security against hacking attempts. OneSign also helps manage account lifecycle issues by enabling administrators to force password changes to applications on a more frequent basis. OneSign reports can provide detailed usage statistics detailing which network log-ons are being used as well as the last time an SSO-enabled application was used. Extensive built-in reports can provide the administrator with broad and deep visibility into how the various applications are being used and by whom, as well as when application credentials were changed.

*Reduce risk with multi-factor authentication.*

OneSign supports a range of strong multi-factor authentication methods, whether used solely or in combination, including: OTP tokens, finger biometric identification, proximity cards (active or passive), and digital certificates. The use of strong authentication ensures a higher confidence that the correct user is accessing the system. Organizations that deploy OneSign Physical/Logical have the added security of knowing that a user is accessing the system from a known location.

*Enforce electronic transactions using strong authentication.*

OneSign's ProveID feature allows organizations to build transactional strong authentication right into any application's workflow via a simple API call to the OneSign Agent. ProveID, in combination with any application, can ensure transactions are properly and traceably authenticated, eliminating compliance and policy risks, including unauthorized data transfers, complicated workflows and illegitimate or erroneous transactions or activities.

*Automatically suspend or remove users no longer authorized to access an IT system.*

If not quickly barred from access, former employees and contractors pose a significant security risk. OneSign reduces this risk in a number of ways. First, OneSign administrators can rapidly enable or disable any user from accessing the network and applications. Organizations with user provisioning systems can give that same power to provisioning managers, because OneSign integrates via industry-standard SPML API to leading user provisioning systems. Organizations that deploy OneSign Physical/Logical have the added benefits that come from integration with leading PACS products. For example, when the Physical Security department revokes a user's badge, OneSign Physical/Logical automatically prevents that user from logging on to the network either locally or remotely, or attempting to access SSO-enabled applications. Finally, OneSign can generate credential-sharing reports; these can be used to discover multiple users who might be using the same application credentials --- especially for administrator accounts.

### ***Integrate physical security and logical (IT) security access systems.***

Signed in 2004, Homeland Security Presidential Directive 12 (HSPD-12) mandates use of smart cards, finger biometrics, and public key infrastructure (digital credentials) in HSPD-12 architectures. By having access to both physical and IT systems based on the same identity data, organizations gain the power to analyze and correlate security events across the physical and IT realms. This enables “location-based authentication” whereby authorized users can only gain access to IT systems when they are in a designated or secure area within a facility. OneSign Physical/Logical supports this practice, providing the benefits of interlocked network/remote access without requiring organizations to upgrade the IT and Physical access systems or to reissue new badges. Instead of requiring dual-credential smartcards, OneSign Physical/Logical leverages the existing investment in the physical access control system, door readers and deployed card to provide additional security afforded by interlocking IT access with physical access. This non-invasive approach provides additional reporting visibility, as well. Security officials can generate a complete access timeline that shows which door the user last entered, the computer that user logged into, and the applications accessed.

### ***Secure access to sensitive networks and applications by limiting access to: valid users with valid credentials; accessing from valid locations; accessing during valid hours.***

With OneSign Physical/Logical, organizations can layer network and remote access policies onto physical access policies around work locations and schedules. Security officials can configure the system to automatically prevent users from logging onto the system if they are attempting access outside their work area or during off-work hours. Because OneSign Physical/Logical links users to their locations, it can spot and thwart log-on attempts made from other locations inside and outside the organization.

### ***Encrypt credentials stored both on server and workstations.***

OneSign keeps all users’ application credentials encrypted both on the client and on the OneSign server using advanced 128-bit AES encryption. This security model extends to not only the persistent credentials stored on the server, but also transient data in transit between the SSO client or in memory data in the client. Early encryption and late decryption ensure a minimal gap when the log-on credentials are available in plain text and provide a dramatic improvement in security over the use of Posit notes for passwords.

### ***BEST PRACTICES IN MONITORING AND REPORTING* Monitor all authentication events, including successful and failed access attempts to networks and applications.**

OneSign generates SYSLOG output for integration with event correlation tools and SNMP traps for generation of real-time notification. Rather than cobble together identity access information from a variety of independent systems and infrastructures, Imprivata’s compliance reporting centrally consolidates all access information in simple-to-run reports that show: a) when a person entered a facility or room; b) when they logged onto a network; c) what applications they accessed; d) when they logged off; and e) when they exited a facility.

### ***Provide audit logs to identify unauthorized activities, detect intrusions, and promote user accountability.***

OneSign’s comprehensive monitoring and logging ensures a complete record of SSO and password policy transactions. User-side logs are consolidated centrally to keep track of which applications were accessed, when, by whom, from which computer. Event logs cover user switching, password changes, login failures, enrollment, and more. Log file maintenance can be automated by the administrator based on file size or other parameters. OneSign’s unique Username Correlation Report can instantly generate a list of all users who are sharing common credentials for any SSO-enabled applications across the enterprise. This is especially useful when an employee leaves the organization and discovers shared accounts. Logs can be read or published in standard SYSLOG format, and logs can be retained online for any specified period of time.

When integrated with a company’s PACS, OneSign interlocks policy for network and remote access to

facility; enforces work area or zone-based network access to critical data; and provides instant user-lockout when a user's badge is revoked.

OneSign also generates incident reports that are time-traceable to the user for: entry/ exit from a facility; authentication to a computer; access to any specific application; and password-related activity within that application.

***Provide reporting and "forensics" that confirm when users are no longer authorized to access a system and automatically remove/suspend user account access.***

OneSign monitors and reports on a broad range of authentication activities, including: individuals logging into the network or a specific application; failed log-in attempts --- by whom, when, and from where; and the type of authentication used.

The ability to place a user's physical presence at a particular computer has tremendous deterrence effect by eliminating the ability to hide behind an electronic log-on. The user can no longer say, "It was someone else using my log-on and password."

***Integrate with Security Information Event Management (SEIM) products.***

OneSign records all user events in a centralized log file, e.g., user log-in, password change, session start/ stop, success/failure events, providing a reporting trail accessible to the administrator. OneSign can be seamlessly integrated with SEIM products via native SYSLOG support. This gives administrators the ability to collect all workstation and application access event information, and react to them in real-time

## **BEYOND COMPLIANCE**

Most regulatory mandates set goals, but very few provide guidance to achieve them. Nor do they take into consideration the potential cost of compliance or its impact on business operations or user convenience or productivity. However, these are issues of major concern to any organization developing a compliance plan. Accordingly, Imprivata has compiled the following list of achievable recommendations that provide best practices guidance that goes beyond compliance.

Ensure deployment costs are reasonable and affordable.

Because OneSign allows organizations to implement SSO without modifying application software, requires minimal configuration, and can be deployed enterprise-wide quickly and easily, deployment costs are affordable for all enterprises, even small- and medium-sized organizations.

***Choose a solution that can be implemented swiftly and easily.***

Organizations can deploy OneSign from a central location using its intuitive browser-based interface. User training requirements are minimal with a short learning curve.

***Ensure ease of administration through centralized management.***

OneSign's appliance form factor extends the ease of use paradigm to not only the packaging but the administrator user interface. All OneSign administrative tasks can be performed by authorized personnel from the browser interface with an Internet connection. Task-oriented functions provide an easy-to-follow metaphor for performing activities related to setting up authentication policies, managing users, enabling SSO for applications, and running reports. Award-winning contextual help information is displayed in a non-intrusive manner, guiding administrative actions.

***Keep cost of ownership low by choosing a solution that requires little ongoing maintenance.***

Once deployed, OneSign requires limited attention. Users can be quickly added, changed, and deleted. The SSO-enabling of new applications is fast and easy. Strong authentication factors can easily be added or changed for individuals or groups. With OneSign, organizations can start simply by deploying Authentication Management, then add SSO protection or Physical/Logical integration if and when they choose, without the need for major hardware upgrades or other disruptions to business.

***Choose a highly-reliable solution that can withstand system interruption.***

OneSign is delivered as a multi-machine load-balanced offering with full distributed, failover, and disaster recovery capabilities. OneSign's web-services architecture increases availability, business continuance, and disaster recovery capabilities. OneSign's distributed architecture leverages a high-performance, transaction-oriented database to serve as the system backbone to manage and distribute security events and audit records reliably over the enterprise.

***Choose a scalable solution to accommodate growth.***

A single OneSign configuration can scale to support an unlimited number of users distributed across multiple locations throughout the world with complete distributed management, delegated administration and business continuity capabilities. Also, since it is web services-based and requires no changes to infrastructure, OneSign can be implemented in manageable increments or extended as the organization grows -- whether organically or through acquisition. OneSign can adapt and evolve as IT demands change.

***Choose a solution that is convenient for users.***

Achieving and maintaining regulatory compliance will not be easy if the effort puts an undue burden on users or equires major changes in user behavior. OneSign is virtually invisible to users, enabling them to support compliance while maintaining, or even enhancing, their productivity. By simplifying password management, OneSign eliminates one of the biggest sources of user frustration -- the need to memorize multiple complex passwords for all the applications they use. OneSign also ensures that users don't get locked out of their applications as a result of incorrect or forgotten passwords, thereby enhancing their productivity.

**ONESIGN: EXEMPLIFYING BEST PRACTICES IN IDENTITY MANAGEMENT**

Today, more than 500 organizations are using OneSign to support these common recommendations and requirements. By providing solutions that are affordable, easy to deploy, and convenient for users,

Imprivata OneSign can help you to deliver security and identity management best practices for your organization.

For more details on Imprivata's Converged Identity and Access Management Platform - OneSign, please visit: <http://www.imprivata.com> or contact Imprivata at: 877-ONESIGN.

## APPENDIX: THE ONESIGN PRODUCT FAMILY

OneSign solutions include:

**Imprivata OneSign Authentication Management** increases network security and simplifies the cost and complexity of network authentication management by replacing Windows and remote access VPN passwords with a broad range of strong authentication device options. These options include integrated management of One-Time-Password (OTP) tokens, finger biometrics, smartcards, and building access cards. Imprivata OneSign can mix and match these various authentication modalities to provide greater employee access security through flexible user authentication management, whether accessed through the network locally, via remote VPN, or while working offline. The industry's most powerful and innovative identity and access management appliance also delivers options for a seamless upgrade to Single Sign-On and/or integrated Physical/Logical capabilities.

**Imprivata OneSign Single Sign-On (SSO)** quickly and effectively solves password management and employee application access issues. Its breakthrough technology helps organizations benefit from increased user productivity and reduced password management costs by enabling single sign-on to all enterprise applications --- legacy, client/server, JAVA and Web. OneSign SSO does not require any custom scripting, changes to existing directories, or inconvenient end-user workflow changes. Companies benefit through centralized password administration, lower help-desk costs, increased user productivity and satisfaction, and ability to demonstrate compliance. With integrated support for multiple, strong authentication methods and centralized password policies, it allows companies to implement levels of security that are appropriate for their environments. Additionally, OneSign SSO's robust reporting capability can track log-in history of all users to each application, furthering the compliance tracking effort

**Imprivata OneSign Physical/Logical** integrates building and network access systems for unified enterprise security management. OneSign makes physical/logical security that is simplified, streamlined yet powerful. Beyond simply leveraging the building access badge, OneSign Physical/Logical consolidates identities between physical access systems and IT directories to enable creation and deployment of a single, converged security policy for allowing or denying network access based on a user's physical location, user role, and/or employee status. OneSign delivers physical/logical security that satisfies complex business requirements. For the first time, events from physical security access systems can now be incorporated into network access decisions, providing a finer layer of authentication for closing security gaps, and providing organizations with broader monitoring and reporting capabilities in order to better demonstrate regulatory compliance.

Imprivata's Compliance Reporting easily reports in real-time an aggregated view of when, how and from where an employee gained network and application access, addressing core access policy requirements contained within many of the regulations discussed in this paper, ranging from PCI, GBLA, Basel II, HIPAA, SOX and other.

By having all access information available at the push of a button via standardized reporting, Imprivata's Compliance Reporting provides critical value in helping organizations rapidly respond to audit inquiries and easily demonstrate adherence to regulatory compliance mandates.



Offices In:  
Belgium • Germany  
Italy • Singapore  
UK • USA

1 877 ONESIGN  
1 781 674 2700  
[www.imprivata.com](http://www.imprivata.com)

WP-CaB-Ver3-0808