

# Laws, regulations and Secure SSO

*A Bull Evidian White Paper*

*SOX, Basel II, HIPAA, LSF,  
21 CFR Part 11 and Secure SSO.*

**EVIDIAN**  
A Groupe Bull Company

**October 2005  
Version 1.1**

## Summary

- Laws, Regulations and Information Systems
- The Requirements Applying to Secure I.S. Access
- Secure SSO: Central to Applying Today's Laws And Regulations

© 2005 Evidian

*The information contained in this document represents the view of Evidian on the issues discussed at the date of publication. Because Evidian must respond to changing market conditions, it should not be interpreted as a commitment on the part of Evidian, and Evidian cannot guarantee the accuracy of any information presented after the date of publication.*

*This is for informational purposes only. EVIDIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*We acknowledge the rights of the proprietors of trademarks mentioned in this book.*

# Contents

---

<b>Laws, Regulations and Information Systems</b>	<b>4</b>
<b>The Law Responds to Pressing Needs</b>	<b>4</b>
Sarbanes-Oxley (SOX): Protecting Investors	4
<i>Loi sur la Sécurité Financière (LSF):</i>	
Corporate Governance	5
Basel II: Minimizing Operational Risk	5
HIPAA: Protecting the Private Data of Patients	5
21 CFR Part 11: Protecting Patients' Lives	6
<b>The Requirements Applying to Secure I.S. Access</b>	<b>7</b>
The Requirement to Define a Security Policy	7
The Requirement to Implement this Rights Management Policy	8
The Requirement to Implement this Access Control Policy	9
Special Features	10
Sarbanes-Oxley (SOX)	11
<i>Loi sur la Sécurité Financière (LSF)</i>	11
New Basel Capital Accord (Basel II)	12
HIPAA	12
21 CFR Part 11	13
<b>Secure SSO: Central to Applying Today's Laws And Regulations</b>	<b>14</b>
SSO Versus Secure SSO	14
Secure SSO Enables Application of the Security Policy	15
A Single Console	15
Applying the Security Policy to the Workstation	15
Adoption by Users	17
<b>Secure SSO Allows You to Meet the Requirements Imposed By Today's Laws and Regulations</b>	<b>18</b>

## Laws, Regulations and Information Systems

---

Corporate information systems are increasingly governed by laws and regulations.

Parliaments and international bodies go beyond straightforward standards, like those issued by the ISO, which have channeled the development of new architectures. In contrast, legislators are focusing increasingly on the relationship between the use made of information technology by organizations, and its impact on operational processes.

In recent years, the laws and regulations protecting private data of existing and prospective customers have been the most high-profile examples of this trend. The growth of e-mail and the application of Direct Marketing methods have reignited the debate at every level.

However, there are many other examples of laws framed by the legislator and applied to information systems.

### The Law Responds to Pressing Needs

When faced with the need to introduce, amend or vote on a law applying to Information Systems, the legislator is confronted by a number of challenges.

- Information Systems lie at the heart of corporate business processes,
- They follow extremely fast technological cycles,
- They are constantly invading new areas.

Legislating in this area is therefore fraught with risk, either because the resulting laws could hold back company growth, or because they could, quite simply, be unenforceable.

This is why the legislator legislates only where there appears to be a real need to protect individuals and property. This is apparent in the following examples.

### Sarbanes-Oxley (SOX) : Protecting Investors

The aim of section 404 of the Sarbanes-Oxley Act of 2002 is to strengthen the internal control procedures applying to financial reporting.

The bursting of the Internet bubble and other financial scandals have had serious repercussions on the capital represented by the pensions savings of many small savers, some of whom have seen their entire life savings wiped out in just a few days. It is precisely to prevent such scandals occurring in the future and to rebuild trust in the financial markets that laws like SOX have been introduced.



### *Loi sur la Sécurité Financière (LSF): Corporate Governance*

The LSF (French Financial Security Act) is an example of local legislation governing the treatment of accounting and financial data. It was adopted by the French parliament in August 2003 in response to the concerns of shareholders following a series of scandals involving major companies. This law sets out to improve the quality of information supplied to shareholders and the public, make directors more responsible for the preparation of annual reports and make those reports more accurate.

As part of achieving this, the CEOs of *Sociétés Anonymes* (Limited Companies) must explain their internal control procedures in the company's annual report. Similarly, the company's auditors must now audit the internal control procedures "relating to the preparation and treatment of accounting and financial information", and include their findings in the annual report.



### **Basel II: Minimizing Operational Risk**

The race to gain market shares may lead a bank to adopt a high-risk strategy. The problem occurs when this strategy is based not on the bank's own equity capital alone, but also involves the use of its depositors' funds. Containment of the ability to take such risks, in combination with the shared application of a common set of rules, is now reducing risk levels.

Against this background, the New Basel Capital Accord (Basel II) sets out to conduct a methodical evaluation of bank capital structures in the context of the operational risks taken.

The information system is now seen as a potential source of operational risk. Securing access to data provides a means of controlling and reducing risk, and therefore improving the competitive position of the financial institution concerned.



### **HIPAA: Protecting the Private Data of Patients**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the healthcare data of American patients. The healthcare information systems operated by medical institutions and social security departments have enabled patient medical data to be centralized in networked systems.

The operational implementation and ongoing use of mechanisms designed to protect medical confidentiality impose major constraints on healthcare information systems.



## 21 CFR Part 11: Protecting Patients' Lives

The automation and computerization of medication lifecycle management processes have, in the past, resulted in the uncontrolled launch of medications. These medications were then offered to patients without having completed the full validation cycle. The consequences were so serious as to result in the immediate withdrawal from the market of the medications concerned.



During the lifecycle of a medication, the pharmaceutical industry is therefore subject to a process that requires submission of the relevant documents to the Food and Drugs Administration (FDA), and controls the procedures used to store these documents. Since these procedures were originally designed to cope with physical documents (chiefly paper documents), 21 CFR Part 11 specifies the rules governing the submission and storage of these documents in electronic form. The reliability of the IT aspects of medication marketing is now governed by a set of laws and regulations.

## The Requirements Applying to Secure I.S. Access

In terms of Information System access, these laws and regulations generally address the security and reliability of access to applications and data. In most cases, the requirements are structured in a similar way, even though they may be expressed differently.



### The Requirement to Define a Security Policy



One of the first requirements is to define a security policy. This may, for example, be built around:

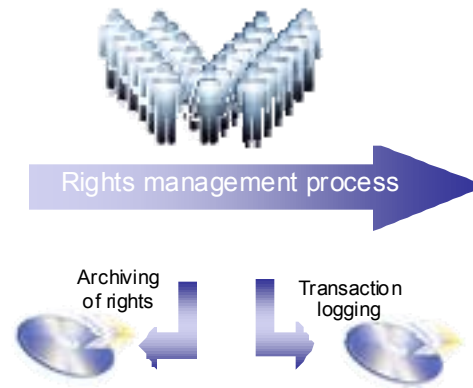
- the classification of data, applications and business processes according to their importance within the organization,
- those of the company's business process profiles subject to access rights and privileges,
- the procedures for allocating profiles and privileges,
- the policies used to authenticate users, and especially those authentication mechanisms described as "robust".

This security policy is defined and implemented with the agreement of the operational departments.

## The Requirement to Implement this Rights Management Policy



Implementation of the access rights management requirements is 3-dimensional.



### Implementation of the Validation Process

The allocation of rights and privileges to a particular user depends on his or her role and position within the organization. Is the user an employee or a sub-contractor? What is his or her position in the management structure? What is his or her job? The answers to these (and other) questions are used to define the list of applications the user may access, and the privileges associated with that access.

The answers to these questions must be given by the various departments, such as the Human Resources Department, the operational departments and even those responsible for managing the partnership.

In general terms, the process of declaring new users and changing user allocations works as well as can be expected, with people explaining their own needs for access authorization. Conversely, the process of de-registering users when they leave is a much less well-controlled process. This procedure is the most risky, since it involves the deletion of user rights relating to people leaving the organization.

### Logging Rights Management Transactions

As with any critical process, the transactions involved in managing user access rights must be logged. This log provides a means of diagnosing the reasons why user rights may have been allocated incorrectly: failure of the process to apply the security policy, failure to apply the process, or even an error in the security policy.

This log maximizes rights management process reliability and facilitates auditing.

### Archiving of Rights

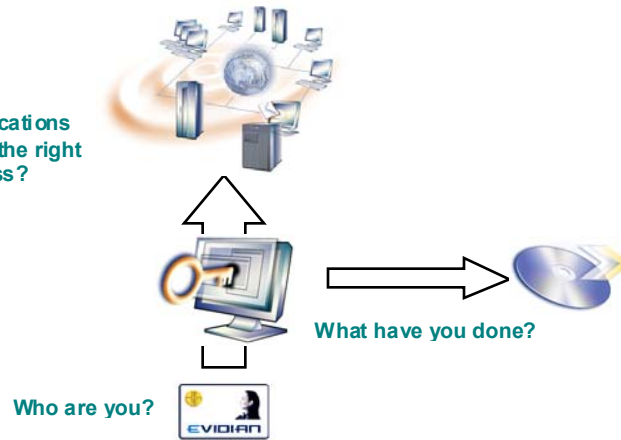
Another dimension is the archiving of active access rights. This archive must supply the information required to analyze individual user rights in the event of a future incident: for example, to identify who had the opportunity to carry out a particular transaction.

## The Requirement to Implement this Access Control Policy

Once the security policy has been defined and user access rights validated, these decisions must be applied to the Information System.



Which applications do you have the right to access?



### Controlling Access To Applications

Access to applications can be controlled at 3 levels:

- By the applications themselves, using their internal access control directory or advanced mechanisms like SAML<sup>1</sup>.
- By a workstation module which, having identified the user, checks that user's rights and restricts access to authorized applications only.
- In a web environment, via a central security gateway or agents embedded in the applications themselves.

#### *Application access logging*

Each access control system must be able to log user access in order to facilitate incident analysis and diagnosis, and the implementation of corrective measures.

The PC module creates a single log file, regardless of whether the target application is web-based or not.

---

<sup>1</sup> SAML is a standard governing the propagation of user identity and privileges to applications. This standard is applied chiefly in the Java and J2EE environments and Service-Oriented Architectures.

### User authentication

Naturally, user authentication is another key area. This authentication may be required on a number of different occasions:

- **Initial authentication**, when the user turns on the PC and enters his or her login name and password for the first time. These are referred to as primary authentication, login name and password.
- **Primary re-authentication**, when the user has to re-enter his or her login name and password to confirm their identity; e.g. after activation of a screen saver.
- **Application authentication**, when a user enters his or her login name and password to open an application. These are referred to as secondary authentication, login name and password.

The security policy may require enhanced user authentication. This enhancement may be applied either to primary or secondary authentication. A number of enhancement methods are available, for example: a compulsory password changing policy, CryptoCards, OTPs and even biometrics.

Applying enhanced authentication to a set of applications in the traditional way may prove extremely costly, or even impossible, since the internal code of each application must be edited to suit the method<sup>2</sup> used.

The PC module addresses all these dimensions (primary and secondary authentication, enhanced authentication and logging) simply and effectively.

### *Authentication logging*

Logging authentication events also contributes to analyzing and improving the processes used to control access to applications.

## Special Features

Each law and regulation sets out the above requirements in its own way, emphasizing either the resources used or results obtained, or even defining a specific area of coverage.

---

<sup>2</sup> Enhanced authentication methods generally use secure communication protocols to establish the identity of a person. So, for example, CryptoCards (or smartcards) use the PKCS protocols of the "PKI" family to provide applications with the ability to check user identity.

## Sarbanes-Oxley (SOX)

SOX focuses primarily on company accounts reporting processes. Naturally, the dependability of these processes relies on the dependability of those concerned with identity and access management: the definition of a security policy, implementation and logging of rights management processes, application access and post-incident analysis, diagnosis and correction.

The requirements of SOX focus on the dependability of accounts reporting processes.



Section 404 of SOX does not contain any specific requirement for Information Systems, but stock market regulators refer to market “frameworks<sup>3</sup>” such as COBIT and ITIL.

To find out more about SOX and identity and access management, you can download our white paper on this subject at:

<http://www.evidian.com/p/am.php?d=wpsox&c=overview>

## *Loi sur la Sécurité Financière (LSF)*

Under the obligations imposed by the LSF, the Chairman of the Board of Directors or Supervisory Board must issue a report on the “internal control procedures implemented by the company” as an enclosure to the annual report.

Although the LSF does not impose a specific methodological framework, or even a precise definition of internal controls, the majority of the largest French companies have adopted the American COSO<sup>4</sup> internal control framework. Other, less detailed, definitions have been issued by MEDEF and AFEP.

Those internal control procedures affecting the allocation of access rights are therefore addressed directly by the LSF. Any significant internal control failure capable of influencing the company’s financial results must be disclosed to shareholders. Amongst the consequences of such a failure, unauthorized access to critical IT processes and changes to computerized accounting data are particularly sensitive issues.



A solution that allocates access rights and monitors access enables the definition of clear, shared procedures, and allows auditors to conduct an internal control audit.

---

<sup>3</sup> Framework: a collection of recommendations and specifications for Information System implementation and management.

<sup>4</sup> “Committee of Sponsoring Organizations of the Treadway Commission”: a private and independent body set up in 1985 under a national commission on financial information, itself a private-sector initiative chaired by James Treadway

## New Basel Capital Accord (Basel II)

Basel II focuses on risk management in financial institutions (including market, customer and internal risks), but also covers those operational risks arising as a result of access to data: human error or embezzlement.

Information technology is not central to the requirements of this accord. However, the implementation of identity and access management processes, their logging for the purposes of analysis, and their addition to the risk monitoring database with relevant indicators all help improve the competitive position of banks.



The requirements of Basel II focus on understanding risk levels, and therefore on the effective control of identity and access management processes. Logging data for monitoring and diagnostic purposes is one of the key points of Basel II.

To take an example of local implementation, the French banking commission issued a questionnaire designed to evaluate the position of financial institutions in relation to the Basel II criteria. Here are some extracts:

- (45) Does your information systems control procedure ensure permanent security of access to assets and data and the procedures used to back them up?
- (31) Does your institution have a database to log losses and incidents?
- (38) Does this report contain alert indicators designed to highlight any increase in risk or any possibility of future losses?

*For more information on Basel II and its implications for identity and access management, you can download our white paper on this subject at:*

<http://www.evidian.com/p/am.php?d=oprisk&c=wpoverview>

## HIPAA

HIPAA targets the protection of computerized patient data in the U.S. by all those organizations likely to handle patient cases: hospitals, laboratories, social security departments, health insurers, etc.



HIPAA takes the standard route of requiring the implementation of a security policy and associated processes.

For example, HIPAA requires:

- Regular analysis of event, access, audit and incident report logs (45 CFR Paragraph 164.308.a.1.ii.D).
- The implementation of procedures to delete all the access rights of employees leaving the organization (45 CFR Paragraph 164.308.a.3.ii.B).

- The use of secure password management systems (45 CFR Paragraph 164.308.a.5.ii.D).

*For more information on HIPAA and its implications for identity and access management, you can download our white paper on this subject at: <http://www.evidian.com/p/am.php?d=hipaa&c=wpoverview>*

## 21 CFR Part 11

The aim of Title 21, Part 11 of the Code of Federal Regulations (21 CFR Part 11) is to ensure dependability of the processes used to validate the electronic documentation of medications.



In addition to implementing the processes associated with a security policy, 21 CFR Part 11 also defines the special requirements applying to authentication, and particularly the obligation for re-authentication when accessing critical resources in order to make certain of the user's identity.

The section covering electronic signature, Chapter 11.200, contains the following points in respect of non-biometric signatures:

11.200.a.1	A signature must employ at least two distinct identification components, such as an identification code and password.
11.200.a.1.i	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
11.200.a.1.ii	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.
11.200.a.2	A signature must be known and used only by its genuine owner.
11.200.a.3	An electronic signature must be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

## Secure SSO: Central to Applying Today's Laws And Regulations

---

### SSO Versus Secure SSO

There are two major principles involved in the SSO concept.

1. **Synchronization**<sup>5</sup> SSO, which uses copy routines to copy the same login name and password into each target system and application.

This type of SSO makes life simpler for the user and makes helpdesk administration easier. On the other hand, it is not a Secure SSO.

In practice, it introduces a security flaw, because if the login name and password are decrypted on a poorly protected system, they can then be used to access even the most critical of applications. To put it simply, you could say that synchronized SSO improves the productivity of your users... and your hackers.

2. The other major SSO principle is based on differentiating the primary identity and password used for initial user authentication, from the secondary identity and password used to enter an application. This is **Secure SSO**. The user only needs to know the primary. To enhance security, this can be replaced by a CryptoCard<sup>6</sup> or OTP<sup>7</sup>-based system. The secondary login names and passwords may be hidden from users.

Differentiating primary and secondary identification in this way enables the definition of a security policy for authentication and its use with all applications, regardless of their specific purpose. That is why this SSO system is usually referred to as Secure SSO.

---

<sup>5</sup> Synchronization SSO may also be referred to as CSO (Common Single Sign-On) and Copy SSO.

<sup>6</sup> CryptoCard: a smartcard with an X.509 certificate, used mainly for authentication.

<sup>7</sup> OTP: One-Time-Password, a single-shot password with a very short validity period.

## Secure SSO Enables Application of the Security Policy

### A Single Console

The Secure SSO management console provides a single point from which to define application access rights. In order to minimize the additional administration involved, this console should use the definitions and organizations already defined in existing directories.

Implementing a Secure SSO requires the organization to put in place a process that terminates in a central user rights management point within the Secure SSO.

#### Where You Can Define Who Accesses What and When

This process enables the controlled definition of “who has the right to access what”: i.e. which user has the right to access which application.

#### Where You Can Audit Rights Management Transactions

These transactions can be logged. It then becomes possible to analyze, after the event, the process that led to an administrator granting a particular user the rights to access a particular application on a particular date.

### Applying the Security Policy to the Workstation

However, the most important point about Secure SSO is the control and reliability it brings to the primary and secondary authentication processes.

#### A Robust Password Policy

Secure SSO uses primary identification to authenticate the user. It can then provide the user with transparent application login management using the secondary login names and passwords.

Logging-in to target applications then becomes a purely IT process requiring no user input.

All that is then required is to implement a robust password policy exclusively for primary authentication.

#### Re-Authentication for Access to Sensitive Applications

Secure SSO can also be used to apply different authentication policies for different target applications. So, as in 21 CFR Part 11, for example, launching a critical application may require user re-authentication. In this instance, Secure SSO requests the user to re-enter his or her primary login name and password.

### Controlled and Audited Delegation of Access

One of the greatest risks concerning the use of login names and passwords is the practice of lending a login name and password. In the practical work situation, where a user has to be absent for a prolonged period, or has to delegate a task, he or she may be tempted to reveal a login name and password combination to a colleague or co-worker.

This most elementary breach of security procedures is hard to combat, because it very often provides a simple and effective way of ensuring continuity of transactions.

A Secure SSO controlled by the company's security policy allows a user to delegate his or her access to another. Secure SSO provides the means to manage this delegation:

- by restricting it to a list of authorized applications,
- by auditing the number of accesses delegated,
- by concealing the primary and secondary login names and passwords of the absent user from the delegated user.

This mechanism provides a simple way of providing operational teams with the resources they need to ensure continuity of transactions even when a team member is absent.

### The Application of Rules Governing "Who Can Access What and When"

The fact that the SSO administrator can check the secondary login name and password for critical applications enables him or her to define and apply the access rules.

So, if the need arises, the rights of a user can be deleted from the Secure SSO system, so that the user concerned can no longer login to critical applications, even where the accounts concerned are still active.

## Adoption by Users

Secure SSO also makes life simpler for users.

### A Single Password (Including Personal Applications)

The SSO relieves users of the need to manage all their own passwords. In practice, when faced with a restrictive password policy, most users resort to workaround strategies that constitute new breaches of security and militate against the original objectives. It is not uncommon therefore to see lists of passwords written down in a book or entered in a PDA.

“Too many passwords kill passwords”.

A robust password policy further escalates this problem.

A Secure SSO solution facilitates user adoption of the robust authentication policy required under the various regulations.

### A Fast ROI to Fund the Project

Where there is no SSO solution, up to 30% of the requests made to helpdesks are about lost passwords. This workload reaches a distinct peak just after the annual holiday period.

The implementation of a Secure SSO solution reduces this workload to virtually zero.

The resulting savings in helpdesk activity help to fund the SSO project.

### Dynamic Use of Workstations

The implementation of an SSO has an unexpected effect on the way users interact with the applications available on their workstations. Freed of the obligation to go through an authentication process every time an application is launched, users can get into the habit of closing applications immediately after use, and re-opening them only when they need to use them again.

This dynamic use frees up PC operating resources, thus delivering an overall improvement in user satisfaction and efficiency.

## Secure SSO Allows You to Meet the Requirements Imposed By Today's Laws and Regulations

---

In general terms, today's laws and regulations cover a sub-set of Information Systems: account reporting applications for SOX, and business process systems for Basel 2, HIPAA and 21 CFR Part 11. An administered Secure SSO lets you focus on these sub-sets and achieve dependable authentication and access control processes. It also enables implementation of the control point demanded by the rights management process.

A Secure SSO therefore allows an organization to meet the requirements relating to identities and access:

**Authentication:** robust initial authentication, followed by secure access to meet the criticality needs of target applications.

**Rights management:** the declaration of user access rights in a directory. This directory can also be used as a single source for the periodic archiving of the rights applying to sensitive applications.

**Implementation:** the adoption by users of the new security policy, and the funding of the project from savings made at the Helpdesk.

Secure SSO is also a first, simple and effective step towards a more generalized identity and access management project. This project will then enable user management and user rights management to be optimized and made more dependable across the entire information system.

For more information go to [www.evidian.com/](http://www.evidian.com/)

Email: [info@evidian.com](mailto:info@evidian.com)