

Identity Management: The Foundation for PCI, SOX, and HIPAA Compliance

Abstract

At the root of most regulatory mandates is the basic requirement to protect information, ensuring its privacy and accuracy. In other words, regulations specify that organizations create an environment of effective overall information security practices. There are many different areas of security, but from a business perspective organizations simply want to prevent misuse of information in order to protect their customers, shareholders, and employees. Building trust and reducing risk can bolster confidence while also helping an organization to meet its compliance obligations.

When most people think of security they think about firewalls and encryption, but one of the most common areas of risk is in an area often taken for granted: the proper management of user and password information. Identity Management is a solution that streamlines, secures, and governs this fundamental business process. This paper discusses the inner-workings of an Identity Management solution and how it relates to these mandates: Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI), and the Health Insurance Portability and Accountability Act (HIPAA).

Introduction

So, what is Identity Management? Identity Management is the collection of processes and technologies that govern the creation, administration, and deletion (Management) of access privileges associated to a given person (Identity) across any number of systems and applications. Identity Management software systems are technical tools that help automate these processes, thereby providing an auditable history of a person's access privileges and the business processes that were utilized to grant, modify, or remove that access. In short, Identity Management systems manage an organization's user IDs and passwords.

You may be reading this and thinking, "Our organization already manages user IDs and passwords." And in all organizations this is true to some degree -- but, how effective and secure is the process? Can your business quickly and easily identify who has access to sensitive applications and data? Who approved that access? Show that it was terminated in a timely manner?

The Problem

Over time, system and application security evolved into a decentralized "silo" model, causing an information security management problem. It was typical to have the personnel supporting each system make the decisions about the security of that system's information independent of any organization-wide scheme; making different persons or departments responsible for the creation and management of user access on each "silo". In most organizations where we have performed Identity Management solutions there are over 40 business applications in use. Most of those applications were selected solely upon their basis to assist in operational efficiency; information security was often an afterthought.

In the typical corporation, the objective is to generate profit for shareholders by selling goods, services, or information that is valuable to the corporation's customers. In the typical "non-profit", the objective is to provide an excellent service which meets a public need without the requirement to earn and redistribute profit. Of course, information security has always been an issue in these organizations, but it has systematically taken a back seat to these higher priority concerns.

Today, several regulatory mandates hold executives accountable for the protection of information in all types of organizations. These mandates include, but are not limited to SOX, PCI, and HIPAA. The recent imposition of these accountability standards requires that the executives of corporations have, and can provide, assurance that sensitive information is protected. Does your organization have confidence in its ability to meet these standards? Is the fragmentation of information security keeping your organization from meeting its obligations?

In most organizations that have not yet embarked upon an Identity Management initiative there are still remnants of the past: decentralized management of user access security, paper based processes, and loose ends which prevent a firm grasp on who has access to the organization's information resources. In most cases this means that generating reports showing which personnel has user access on sensitive systems and applications requires a person to correlate HR reports with individual reports from each system of concern – a tedious and time consuming task. Gathering the access request approvals for these systems may mean following a paper trail into a warren of resource consuming frustration; either searching for that misplaced paper form or performing a cumbersome manual email search. This process is both error prone and lacking the certainty now required by compliance mandates. If an organization can't easily demonstrate who has access to its sensitive information systems, how can the executives be assured that the information is protected?

Let's break this down from a SOX (Sarbanes-Oxley) perspective using a fictitious organization, ACME Co., to make it more tangible.

ACME was founded in 1977 and after a few years realized that managing all of the financials, expenses, and payroll was becoming too cumbersome using paper, and in 1982 they invested in a mainframe. Applications were then developed that ran core business operations through dumb terminals which accessed this mainframe. As the eighties progressed, the personal computer was introduced and began making inroads for specific business requirements at ACME such as spreadsheets and simple word processing; simultaneously ACME had also been growing and opening new offices nationally. By 1992 almost every office worker had a personal computer and local area networks were springing up throughout the organization. Soon after, the network had taken the official position in the organization as the default work tool, and the "client-server" computing model became the next "best thing". ACME then expanded the MIS department and much of the user administration tasks moved to Help Desk. Of course, ACME was now managing mainframe application IDs, Network logon IDs, Internal email accounts, Distributed Server IDs, Database IDs, and Client Server application IDs.

1996 - Suddenly, the Internet shows up in corporate America. In order to remain competitive ACME begins a slow and steady course towards setting up web based interfaces to new and legacy applications for customers, partners, and suppliers. Like most companies at this time, ACME is interested in managing their budget and delivering the most business functionality; application security is an afterthought. This practice resulted in a login provided to a different table, file, or directory for every application. In 1999/2000, ACME is the proud owner of 37 different applications running across 7 platforms, 76 servers, and 2 datacenters with 6 different types of persons requiring access. I'm sure we all recall the scramble for Y2K fixes...

Shortly thereafter, Enron, Tyco, and WorldCom executives systematically manipulate employees and shareholders, dissolving public confidence in the corporation and the accounting firms which were supposed to ensure that public confidence. The main line of defense taken by these executives was that they did not know what was going on in the companies that they were responsible for.

Enter Sarbanes-Oxley (SOX), creating instant accountability for the C-Level Executives who had previously looked at IT like any other operational aspect of a corporation, as a cost center. All of a sudden executives became responsible for ensuring the integrity of their financial data, or else be held personally liable for large fines and even jail time.

In order to restore confidence in corporate America (and to stay out of prison), finding out the answers to the following questions became of paramount importance: Who has access to all of these sensitive financial systems? Who approved access to these systems? What financial information is on the network environment? Are we sure that nobody has access to this information that is in an inappropriate job function; or worse, left the company? Good questions-- but how can the answers to them be produced?

The Solution

Identity Management can solve many of these problems and help an organization comply with regulatory mandates. An Identity Management system is a very specific solution which will provide five main services governed by programmatically enforced policies, helping organizations to improve security and comply.

- 1) **Integration with a "System of Record"** – the appropriate source of person information in an organization is the place where it originates and where it is most likely to be kept up to date. This is typically an HR or Payroll application for employees. When an Identity Management system is integrated with a system of record, the person and job information is fed directly from the system of record. Leveraging the person information from a system of record ensures the following:
 - a. Name spelling errors are handled and name information does not need to be re-keyed which streamlines the process and eliminates the need for many paper forms.
 - b. Job related information is provided, in an ongoing fashion, from the source so that it can be used to enforce policies about who gets access to

sensitive systems. For example, a person moving out of a finance department can have access to financial systems removed automatically.

- c. Person status (active, leave, terminated) is provided programmatically, in a timely and ongoing manner from the source so it can be used to automate actions such as de-activating all access immediately on termination.

2) Provisioning – the Identity Management system will actually perform the user ID creation, modification, and deletion on the systems and applications being managed by the Identity Management system. This is all initiated from a web-based interface providing a centralized view of the systems and applications available in the organization. The interface can be leveraged in a request based fashion by managers or end users, it can be used in an automated role-based fashion based on job function, or perform critical functions according to the needs of Information Security. Leveraging the provisioning feature ensures the following:

- a. Name information on user accounts flows from the Identity Management system and reduces re-keying and mistyping.
- b. User ID naming standards are enforced centrally.
- c. User ID ownership is accounted for by the Identity Management system, ensuring that user IDs are not shared.
- d. A web based interface standardizes the access administration process, facilitates cross-training, and reduces paper.
- e. Time to provision access is dramatically reduced, increasing productivity and end user satisfaction.

3) Workflow – The Identity Management system provides automated facilities for routing approval requests easily and securely. These approval requests can be extensions of user ID access requests, recertification, or almost anything else that can be imagined, as Identity Management workflow engines are highly customizable. Recertification is the process of periodically validating that a person still needs access to a specific system or application through an approval workflow involving the person's manager, the owner of the ID, or anyone else pertinent. The workflow engine ensures the following:

- a. User ID access requests that require approval have an automated approval workflow.
- b. The request approval is tracked relative to the access request.
- c. Periodic recertification of access can occur to revalidate highly sensitive areas of the business, or to catch persons where the Identity Management system was not integrated with a system of record, which is common with itinerant workers such as contractors.

4) Password Management – the Identity Management system provides centralized password policies, password reset self-service through challenge response questions, and password synchronization. Although people frequently talk about biometrics and other multi-factor authentication schemes, the fact of the matter is that the vast majority of all access is granted through a password. Passwords that are properly used and enforced through an Identity Management system ensure that:

- a. Password rules (length, history before reuse, special characters) are enforced centrally.
 - b. Password changes (the fact that the password was changed, not the actual user password) are tracked for audit purposes.
 - c. Password self-service and challenge response moves an expensive burden from helpdesk and places it with the end user.
 - d. Password synchronization increases the probability that one complex password will be remembered, reducing the risk that passwords are written down on easily found sticky notes.
- 5) Audit** – the key part of compliance is the ability to prove that the organization actually enforced its information security policies. This makes the audit and reporting features of an Identity Management system indispensable in any organization. The audit features ensure:
- a. The organization can easily report on who (Persons) has access to what (applications or systems).
 - b. The organization can easily report on who approved specific access requests.
 - c. The organization can easily report on who “recertified” that access for a particular person is still required for specific systems or applications.
 - d. Orphaned user IDs (IDs that do not have an owner, but still exist) can be identified through reporting and eliminated by being deactivated or assigned to the appropriate owner.
 - e. Termination reporting can help demonstrate that access is deactivated when the system of record person status was changed to “terminated”.
 - f. The organization can easily report on password change actions.

The Benefits

Identity Management provides many information security, audit, and user satisfaction benefits, as outlined above. In addition there is usually a return on investment in less than three years, and the compliance benefits abound. The tables below list the requirements of some of the key compliance mandates affecting many businesses right now, correlated with how Identity Management can assist in complying with the requirement.

SOX 404

SOX section 404 requires that the integrity of financial data be certified by executives, and that regular audits take place. This is to ensure that financial statements are not impacted by incorrect or manipulated data. Corporate Executives are held accountable through fines and other criminal consequences. The reports that are produced can be reviewed by the SEC.

| Compliance Requirement | Identity Management Feature |
|------------------------------------|---|
| Ensure Integrity of Financial Data | <u>Provisioning</u> - can ensure that critical data can only be accessed by authorized personnel whose jobs require such information on a “need to know” basis. |

| | |
|---|--|
| Provide audit reports of “who has access to what, and who approved that access” | <u>Audit Reporting</u> - can prove that only appropriate persons have access and that all access was approved. |
|---|--|

PCI

The Payment Card Industry’s Data Security Standard v1.1 was created by a collaborative group of five major credit card associations – VISA, MasterCard, American Express, Discover and JCB – that banded together to form the Payment Card Industry Security Standards Council in 2004. Unlike SOX and HIPAA, which are enforced by the government, PCI DSS is enforced by the credit card associations, with fines and other consequences for non-compliance varying from one credit card association to another. The level to which an organization must demonstrate compliance varies greatly depending on the number of transactions processed per year, however, it is important to note that even the smallest of firms will be held to the highest reporting level with just one security breach. There are 12 major standards outlined in PCI DSS v1.1, and a pervasive and effective Identity Management solution is imperative in creating a fully compliant security solution. Of the “big 12,” five of the standards call for strictly controlled access that can be assisted by Identity Management.

| Compliance Requirement | Identity Management Feature |
|--|--|
| Restrict access to data by business need-to-know | <u>Provisioning</u> - can ensure that critical data can only be accessed by authorized personnel whose jobs require such information on a “need to know” basis. |
| Assign a unique ID to each person with computer access | <u>User ID Ownership</u> - in an Identity Management system a person is associated with, or “owns” each user ID, assisting in eliminating the shared user ID problem. |
| Do not use vendor-supplied defaults for system passwords and other security parameters | <u>Centralized password policy</u> - enforcement can ensure that strong passwords are used on managed applications and systems. |
| Protect stored cardholder information | <u>Workflow with recertification</u> - can make sure that persons no longer requiring access or no longer associated with a company are deactivated from applications or databases housing cardholder information. |
| Track and monitor all access to network resources and sensitive data | <u>Audit Reporting</u> - can prove that only appropriate persons have access and that all access was approved. |

HIPAA

The Title II section of the Health Insurance Portability and Accountability Act was issued in 2003 with a set of varying compliance dates, phasing in by 2006. The goal of Title II, and specifically the “Security Rule” was to promote the use of electronic medical records

over paper, in order to increase the efficiency of the US healthcare system. The general fear among critics of the switch to electronic records was not so much that someone would steal your records and tell your neighbors all of your problems, but rather the fear of misuse of a centralized medical record database by insurance companies in order to deny coverage. In order to achieve the trust of the public and its representatives, the “Security Rule” sets out compliance requirements for electronic medical records with fines and jail time for violators.

| Compliance Requirement | Identity Management Feature |
|---|--|
| Only those with a “need to know” should have access to electronic private health information | <u>Provisioning</u> - can ensure that critical data can only be accessed by authorized personnel whose jobs require such information on a “need to know” basis. |
| Implement procedures to regularly review records of information system activity, such as audit logs, access reports | <u>Audit Reporting</u> - can prove that only appropriate persons have access and that all access was approved. |
| Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends | <u>Integration with a System of Record</u> – provides completely automated termination processing. Also, from the Identity Management Console itself, a person can easily be identified and all of their access deactivated immediately. |
| Implement procedures for creating, changing, and safeguarding passwords | <u>Identity Management</u> – is a solution that governs this exact process |
| Assign a unique name and/or number for identifying and tracking user identity | <u>User ID Ownership</u> - in an Identity Management system a person is associated with, or “owns” each user ID, assisting in eliminating the shared User ID problem. |

Conclusion

Identity Management streamlines and protects the user ID access request, approval workflow, and provisioning process. Identity Management’s integration with systems of record and the provisioned systems and applications provides the missing link in the access management process of most companies. Identity Management’s ability to offer self password management and synchronization also provides a significant reduction in the helpdesk burden, which helps in building return on investment.

Since the appropriate management of access to information is part of a good overall information security program, Identity Management helps organizations comply with regulatory mandates requiring the certification of good information security practices. Identity Management audit reporting provides the proof that the organization is a good steward of the sensitive information under its control.

Call to Action – Where to Begin

It is clear that IT systems, particularly those that house or process sensitive data, are under the microscope of federal, state, and industry bodies forcing them to comply with ever-changing standards. In addition to these oversight bodies, consumers are no longer in the dark about the threat of identity theft and are beginning to use the force of their wallets to demand compliance. Compliance is no longer an option, but rather a necessity in maintaining true competitive advantage in the marketplace. The question has moved from “should we comply?” to “how do we comply?”

The first and most important step in creating a truly compliant environment is the assessment of current systems and business processes within the corporate environment. Professional consultants specializing in Identity Management can be invaluable allies in the quest to improve security posture and become compliant.

Kyle Watson is the founder of Watson SCS, Inc. - a premier IBM business partner for Identity and Access Management security solutions, often delivering security solutions on behalf of or along side IBM. Watson SCS offers IT Security Access Administration Assessments for companies concerned about the security of their computer systems and those struggling to comply with strict regulations. For more information, please contact Watson SCS at (866) 805-6066.

Copyright © 2007 Watson SCS, Inc. All rights reserved.