

## WHITE PAPER

---

# Identity Management: A Growing Player in the Regulatory Compliance Challenge

Sponsored by: HP

---

Christian A. Christiansen  
February 2005

## IDC OPINION

Since the mid- to late 1990s, and in response to corporate scandal and increasing concerns about data theft and tampering, global lawmakers have implemented a series of wide-ranging compliance regulations to protect investors from poor corporate governance and consumers from unauthorized use of their private information.

These regulations dramatically affect many enterprises and may require them to find the many paths to compliance through policy, process, and technology. The result is changing the way global firms are conducting business, and most firms are keenly aware that noncompliance now is much more risky than in the past, even as they struggle to understand which of the possible paths is the best to take.

Risks include substantial civil penalties and, in some cases, criminal prosecution. Therefore, enterprises are evaluating a wide range of IT security technologies to enable cost-efficient compliance. IDC believes that of the myriad technologies available, identity and access management (IAM) solutions offer a solid answer to handling compliance regulations pertaining to authorization, authentication, audit, and privacy/protection of personally identifiable information.

---

## Approach

IDC wrote this paper during fall 2004. Based on historical and current research, we talked to customers and vendors affected by information and data laws in the United States, Canada, and Europe.

To reflect customer opinions, IDC conducted in-depth interviews with executives who are familiar with privacy compliance issues and IAM solutions. With HP's help, IDC interviewed large firms from several industries that are focused on implementing solutions specifically designed for compliance with regulations. In these open-ended discussions, we listened to customers' external business concerns, internal organizational problems, and solutions to address current and future compliance regulations. IDC focused this paper on the enterprise customers' need to understand specific regulations and develop appropriate compliance solutions.

This IDC white paper:

- ☒ Looks at seven regulations
- ☒ Illustrates where enterprises should be attentive to the impact on their own organizations
- ☒ Offers "best-practice" solutions with a corresponding technology feature set

### ***Regulations Covered in This White Paper***

This white paper is designed to be read in sections. It may contain a certain amount of redundancy because it permits readers to reference only the regulations most pertinent to them. The regulations covered by this white paper are as follows:

- ☒ Sarbanes-Oxley (SarbOx)
- ☒ Health Insurance Portability and Accountability Act (HIPAA)
- ☒ Personal Information Protection and Electronic Documents Act (PIPEDA)
- ☒ Gramm-Leach-Bliley Act (GLBA)
- ☒ European Union Privacy Act (EUPA)
- ☒ California Senate Bills 1386 and 1950
- ☒ Japanese Personal Information Protection Act of 2003 (JPIPA)

IDC recognizes that these regulations are only a subset of worldwide compliance legislation. We chose to focus on these regulations because we believe they affect the largest number of corporate entities and their customers.

## **SITUATION OVERVIEW**

With the Internet accelerating the sharing and collecting of information of all types, concerns about the accuracy and protection of the collected data have grown drastically. Privacy concerns and corporate financial scandals (e.g., Enron, Tyco, Adelphia, Parmalat, Eli Lilly) have led legislators around the world to respond to their electorates and the many worldwide investors that were financially devastated by governance failure and identity theft.

Such cases have raised serious questions about the accuracy and protection of data. These situations have resulted in an increase in legislation and regulations enacted by various governments throughout the world focusing on the prevention of overt and inadvertent abuses of the data collected and managed by companies. Enterprises both large and small are suddenly awash in a sea of regulations — some of which they might not yet be aware — and wondering what they will need to do to become compliant to avoid the somewhat stringent civil and, in some cases, criminal penalties.

## **IAM and Compliance**

Clearly, managing regulatory compliance for today's enterprises requires both process and technology. As the cost of noncompliance rises in both legal and criminal responsibilities, the imperative to understand and efficiently respond to requirements increases in importance. IDC believes that well-implemented IAM products can help companies meet many compliance requirements.

A large portion of protecting information in a system relates to how well access to that information is controlled; that is, knowing who is accessing the system and when and confirming that the people who are accessing the information really are who they say they are. Enter IAM systems. While fulfilling the important goals of controlling and monitoring access to certain data resources, IAM systems often have the ability to do much more because they have features that drive business value as well as provide the required compliance.

### ***Business Drivers: Moving Beyond Basic Compliance***

Although regulatory compliance itself can be a compelling reason to deploy new systems and processes, it is important to understand the business benefits that can make the addition of new, or augmentation of old, systems more palatable and reasonable for corporate decision makers. IDC research has identified a number of positive benefits that enterprises might derive from introducing IAM systems beyond that of simple compliance with government requirements:

- ☒ **Improved corporate oversight.** Applicable to both internal (e.g., acceptable use policies) and external (e.g., regulatory compliance) exposures, corporate oversight can provide corporate executives with a single view of the level of compliance, potential violations, automated/semiautomated policy implementations for preventing violations, and protection against failed audits.
- ☒ **Efficient provisioning of user access.** Getting users access to the right information they need to do their jobs quickly and accurately greatly reduces the time users spend waiting for access.
- ☒ **Instant termination of rights.** When an employee/business partner/contractor/supplier relationship ends, companies must ensure that the access rights of individuals involved in such a situation are revoked immediately.
- ☒ **Secured user access to internal resources.** This benefit allows users to work anywhere, anytime, thereby increasing their productivity on the road.
- ☒ **Fewer exploits from unauthorized access.** Preventing unauthorized users from tampering with and taking down systems decreases the risk of opportunity cost due to unplanned downtime.
- ☒ **Delegation of lower-level tasks.** Delegated administration enables IT to focus on more important tasks and let users manage their own accounts and rights as well as provision access where required. As a result, IT staffs can address more important and business-critical needs.

- ☒ **Distribution of labor.** This benefit allows for delegation of responsibility and accountability down the hierarchy so that individuals can focus on the most important tasks.
- ☒ **Reduced cost of technology.** Increasing the efficient use of technology resources, such as databases, by the consolidation of information into one secure location leads to greater efficiencies in storage and networking resources.

***Regulatory Commonalities***

Business benefits and drivers certainly will help enterprises justify the expense of achieving compliance, but it is also worthwhile to know which requirements are core to most regulations. Thus, enterprises can plan accordingly if they are subject to more than one regulation or if they need to ensure that their systems are capable of expanding in the future. To that end, enterprises would be wise to understand the foundation of common requirements among the more well-known regulations. Table 1 reviews the requirements common to the regulations covered in this white paper and the technology features or systems that address the requirements. Although it is not a specific requirement of regulations, having a common infrastructure on which the various supporting systems are run will aid the transition to new/upgraded features as laws continue to evolve.

<b>TABLE 1</b>	
Common Technology Features for Addressing Regulatory Requirements	
Regulation Requirement	Technology Feature
Restrict access to sensitive data	Authentication and authorization system
Protect sensitive data from unauthorized access	Authentication and authorization system
Track, audit, and report on user and IT administrative activity	Audit and reporting system

Source: IDC, 2005

Tying business drivers into compliance enables companies to identify greater efficiencies in their compliance efforts and moves organizations toward "business-driven, services-oriented identity management." Furthermore, by starting with a common infrastructure for complying with government regulations, organizations are prepared for future expansion of compliance to other regulations as the business matures.

In looking to vendors that supply IAM systems, we note that HP provides a strong example of a vendor with a product line that not only can fulfill compliance needs but also can provide additional features for increased business value and help prepare organizations for compliance with future expansion and regulation coverage.

## HP OpenView Identity Management Solution

IAM systems can provide a best-in-class solution to help organizations achieve compliance with government regulations that require protection of private and sensitive information from theft and tampering. These systems provide companies with an integrated way to manage and control the access, rights, and other aspects of an individual user's identity. Enterprises that integrate IAM solutions into their networks gain a system that can control and manage access to all network resources, including those containing the most sensitive data under regulation.

A system such as HP OpenView Identity Management can provide the business service identity management required by clients to meet both regulatory and business requirements. HP's IAM solution provides best-in-class features to meet the needs of its clients and comprises three products:

- Select Access
- Select Identity
- Select Federation

These three products work together to enable enterprises to comply with regulatory demand while gaining business efficiencies and value in the process. Targeted directly at core compliance issues, HP's IAM solution helps organizations address the challenges of increased regulations.

**HP OpenView Select Access** allows for management and tracking of an individual user's single sign-on access and movement history within an organization's network. All activity is audited and may be reported upon in short order if needed.

**HP OpenView Select Identity** works in concert with Select Access to make sure that users logging into the network, onto a server, or to an enterprise application (e.g., customer resource management) are actually who they say they are. Select Identity automatically provisions the resources that users need, helping to eliminate errors and potential for unauthorized access that often come with manually provisioning large numbers of users for large numbers of resources.

**HP OpenView Select Federation** is designed to govern and audit federations of companies, including the ability for smart user provisioning and privacy management.

Table 2 identifies the features provided by the HP OpenView Identity Management solution.

A system such as HP OpenView Identity Management can provide the business service identity management required by clients to meet both regulatory and business requirements.

**TABLE 2****Features of the HP OpenView Identity Management System**

Feature	Description
Delegated administration	Allows for the delegation of identity management tasks (e.g., password reset or requesting new applications access privileges) to some or all of the user profiles; policies and audit functions enable tracking of activities.
User self-service management	Allows users to enroll and manage their profiles independently and automatically assigns data and network entitlements based on the information the users submit at the time of enrollment.
Consolidated auditing system	Provides a consolidated security audit trail for all access requests; authorization decisions and administrative changes are logged. Audit entries are digitally signed and allow system administrators to recall significant events such as the number of failed attempts to access a certain resource.
Reporting	Creates customer reports to provide insight into the operations of the system. Third-party report analysis tools may also be used.
Real-time alerting	Allows definition of alert levels, handling instructions and lists of recipients for alerts according to internally developed policies. Components may be monitored and managed with HP OpenView Operations and tracking and alerting of events, such as self-service password reset and new user provisioning, can be provided through HP OpenView Service Desk. Alerting and tracking can help with regulatory compliance by alerting for specific activities such as unauthorized access attempts to restricted resources or failed logins, for example.
Performance-based scalability	Scales with increasing number of applications and manages spikes in user activity. Entire architecture is replicable. Workload balances across multiple policy servers in case servers go down.
Provisioning	Automates the creation, maintenance, and termination of user accounts and entitlements, thereby reducing the risk of "orphan" accounts that could be spoofed by hackers or unethical employees.
Workflow, audit, and reporting	Provides a method to model business processes, including implementing and automating approvals. Approvers may accept, reject, or comment on the request. The work can be designed to integrate with external non-IT processes such as creating work orders in HP OpenView Service Desk to procure a desk and a phone for a new employee. Audit and reporting features provides information on who has access to what resources within the organization.
Single sign-on	Enables a seamless user experience when navigating between multiple resources. Allows business partners to securely connect across corporate boundaries, including separate user databases and authorization processes.
Password management	Defines and enforces password policy, automates password resets, and synchronizes passwords on disparate information systems.
Automated discovery	Automates the discovery and importing of existing users, profile information and access rights and new resources are brought online.
Variable entitlements	Manages exceptions to role-based entitlement without adding more roles or rules.
Extensible connector architecture	Ensures provisioning connectivity to present and future IT environments as current compliance regulations change and new ones are adopted.

Source: IDC, 2005

These features enable HP's IAM solution to meet the needs of a wide range of regulations. The next section of this white paper is devoted to the seven regulations chosen for this paper and the requirements they exact upon the covered enterprises.

## THE REGULATIONS

Complex regulations increasingly drive senior management's concerns about the accuracy and protection of sensitive and private data, such as:

- Financial history
- Credit reports
- Bank accounts
- Medical records
- Social security numbers
- Account names and numbers
- Occupation and employee number

However, this list represents only a small subset of vulnerable information. The wealth of available information sparks ongoing debates regarding what data is considered private and what data is considered public. The regulatory compliance legislation was created, in many cases, to end some of these debates by better defining private and public information and its use.

Although the regulations may range in focus from specific (affecting companies in a single industry) to broad (affecting all companies), they share a number of commonalities as mentioned above. In this white paper, we review seven regulations targeted at protecting the accuracy and privacy of data collected, managed, and reported upon by corporate entities. Table 3 summarizes these regulations.

**TABLE 3****Brief Descriptions of Selected Privacy Regulations**

Regulation	Brief Description
SarbOx	Sarbanes-Oxley redesigned the accountability requirements for corporate governance officers, requiring CEOs and CFOs to certify their companies' financial results and be held personally accountable for the results. The penalties are now much more severe and carry both criminal and class-action suit potential. Sarbanes-Oxley is aimed at preventing, or at the very least deterring, corporate scandals such as those of MCI and WorldCom. Thus, corporations will be accountable for their numbers and required to implement a series of internal audit and self-assessment tools to ensure compliance.
HIPAA	HIPAA regulates the protection, portability, and privacy of an individual's medical information. It impacts organizations that maintain health information as well as their partners and vendors. Medical information is highly sensitive, and the potential for abuse of that data is extremely high. The act requires organizations to protect information from security violations and correct any problems if violations occur.
PIPEDA	Much like HIPAA, PIPEDA prohibits the collection, storage, and disclosure of personal information related to an individual without that person's explicit consent. Personal information is any factual or subjective information, recorded or not, about an identifiable individual. PIPEDA provides the individual with the right to know what is being collected and change the information if it is inaccurate. Interestingly enough, U.S. and U.K. businesses may also be bound by the rules protecting Canadian citizens' personal information.
GLBA	Specifically targeted at the financial industry, GLBA protects the personal and private data of bank and financial institution customers from internal and external threats or hazards as well as the unauthorized use of said data.
EUPA	EUPA focuses on ensuring that member states require the prohibition of collection of certain data and provide stringent protections for the data that is collected. This act, however, doesn't provide any punitive measure for noncompliance. Rather, it requires the member states to provide the punishments. It is applicable to all businesses regardless of industry, size, and shape.
CA SBs 1386 and 1950	CA SB 1386 applies to companies that do business in California — whether or not they have physical locations in the state. Its main stipulation is that all businesses must disclose the breach of any personal and private information as it pertains to California residents. It contains no criminal or civil penalties, but it does permit class-action lawsuits. SB 1950 expands SB 1386 by requiring that all businesses in possession of California resident data provide reasonable security procedures and practices to protect the information and receive a contract from any third parties with which they share the personal and private information that stipulates the maintenance of reasonable security practices on the part of the third parties.
JPIPA	JPIPA bumbled with several fits and starts before finally being passed in 2003. Much like its Western counterparts, JPIPA focuses on the protection of individual personal and private information from abuse, theft, and misuse. The biggest contention with this act was that it almost eviscerated the freedom of the press. Provisions for press and journalistic rights were finally included, but the overall act itself is more stringent than many.

Source: IDC, 2005

These regulations apply to North America, Europe, and Asia, as evidenced in the brief descriptions above. However, while some regulations, such as HIPAA, target specific industries, others, such as CA SBs 1386 and 1950, target all businesses that are collecting information and doing business in a specific location. Determining which regulations require compliance and their corresponding scope of coverage is a confusing — yet vitally important — process for organizations. Table 4 identifies the regulations and their scope.

**TABLE 4**

## Regulatory Impact on Specific Industries

Regulation	All Businesses	Financial Services	Insurance	Banking	Healthcare	Pharmaceutical
SarbOx	X					
HIPAA			X		X	X
PIPEDA	X*					
GLBA		X	X	X		
EUPA	X					
CA SBs 1386 and 1950	X					
JPIPA	X					

\* Compliance is required for private sector companies only. Public sector companies do *not* have to comply.

Source: IDC, 2005

The regulations themselves often do not stipulate a technology requirement as a solution (although some do suggest technological solutions), but IDC believes that strong IAM solutions can help organizations protect the information for which they are responsible. As noted above, IAM solutions focus on validating that users are who they say they are and that they have access to the appropriate data and resources. Regulations often require organizations to prove their diligence in protecting information through audits. A strong IAM solution such as HP's also provides organizations with the ability to track and report on user activities as well as a host of other internal and external events that could jeopardize their ability to keep their sensitive data and information safe from theft and tampering.

The following sections review seven regulations and their IAM requirements; provide IDC's best-practice solutions; and include correlating HP examples of how those best practices would be put into play. The regulations are reviewed in brief above, and subsequent sections provide in-depth details about how they impact the need of organizations to deploy IAM solutions. These seven regulations are Sarbanes-Oxley (SarbOx), Health Insurance Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Documents Act (PIPEDA), Gramm-Leach-Bliley Act (GLBA), European Union Privacy Act (EUPA), California Senate Bills 1386 and 1950 (CA SBs 1386 and 1950), and Japanese Personal Information Protection Act 2003 (JPIPA).

The purpose of this paper is to focus on the regulatory compliance issues that deal with IAM, and therefore we have broken the document into sections that review each regulation and its particulars. Because this paper is structured in parts, some information redundancy may occur between sections.

---

## **Sarbanes-Oxley Act of 2002 (SarboX)**

The Sarbanes-Oxley Act of 2002 rose out of the ashes of the Enron and WorldCom accounting scandals. SarboX is best known for its ability to hold CEOs and CFOs accountable for the accuracy of their organizations' financial results. Inaccurate finances can expose executive management to potentially severe penalties — such as jail time and class-action lawsuits. The passing and subsequent enacting of SarboX created a flurry of accounting restatements, shifting of executive ranks, and almost desperate corporate need to understand what IT requirements need to be in place to make the audit process of SarboX less painful for organizations.

Specifically, Section 404 of SarboX requires the Securities and Exchange Commission (SEC) to publish and enforce rules for implementing internal controls to ensure the "accuracy and transparency" of public companies. In turn, the SEC is requiring the following information from corporate entities in their annual reports:

- Management must assume responsibility for establishing and maintaining internal control over the company's financial reporting.
- Framework used by management to evaluate the effectiveness of internal controls must be identified.
- Effectiveness of internal controls must be evaluated at the end of the company's fiscal year.
- Auditor must have independently assessed and approved the internal controls.

SarboX requires the identification of all important financial accounts, the business processes related to those accounts, and the IT infrastructure that is involved with those processes. Accounts, processes, and infrastructure must be able to provide a trail of who accessed what data and when. All the data must be accurate and double-checked for tampering at any level. Table 5 identifies the requirements that SarboX makes upon those it regulates, IDC's best-practice solutions, and the corresponding features in HP's IAM solution.

**TABLE 5****Identity Management Requirements of SarbOx**

Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Management and tracking of access to sensitive financial data	Centralized identification and authorization system	Single sign-on support, provision/workflow/reconciliation
Efficient management of who has access to sensitive financial data	Comprehensive workflow and user management system	Workflow, delegated administration, automated user/resource discovery
Audit and reporting features for tracking and reporting on user logins and access requests	Robust audit and reporting system	Audit system with reporting and real-time alerting features
Need to ensure responsibility and accountability of management	Delegation system	Workflow, delegated administration

Source: IDC, 2005

### **Health Insurance Portability and Accountability Act (HIPAA)**

Much like SarbOx was created in response to financial abuse, HIPAA was created in response to the abuse of private patient information by medical companies, whether or not such abuse was maliciously intended. Prozac manufacturer Eli Lilly is one of the best known cases, but certainly not the only example, of inadvertent abuse.

An Eli Lilly employee wrote a simple program to automate the sending of an email to subscribers of an online newsletter about Prozac. A mistake in the programming code of the newsletter placed 669 client names in the "To" header of the email, essentially exposing the identity of those 669 people to each other. Eli Lilly was found guilty in court and not only forced to pay restitution but also required to submit to permanent ongoing audits of its systems to ensure the protection of its consumers' data.

HIPAA specifically targets healthcare professionals and their vendors, partners, customers, and business associates. One section — the Privacy Rule — explicitly deals with protecting the privacy of individual information. This rule stipulates that a covered organization must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. The Privacy Rule pertains to both electronic and nonelectronic (e.g., paper-based and verbal) information. Medical companies, as well as their business partners and vendors, must be able to show absolute proof of their protection of and limitation of access to patient data from both internal threats (employees making mistakes or stealing information) or external threats (hackers stealing information). Table 6 reviews the requirements of HIPAA's Privacy Rule, IDC's best practices, and HP's solution to the challenge.

**TABLE 6**

## Identity Management Requirements of HIPAA

Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Management and tracking of who has what access to personal and private information	Centralized identification and authorization system	Single sign-on support, audit and reporting with real-time alerting
Efficient management of who has what access to personal and private individual data	Comprehensive workflow and user management system	Workflow, delegated administration, automated user/resource discovery
Audit and reporting features for tracking and reporting on user logins and access requests	Robust audit and reporting system	Audit system with reporting and real-time alerting features

Source: IDC, 2005

### **Personal Information Protection and Electronic Documents Act (PIPEDA)**

The Canadian PIPEDA is a new law directed at governing the information held by private sector organizations, and it specifically deals with information collection, use, and disclosure. It incorporates as a schedule the Canadian Standards Association Model Code for the Protection of Personal Information, and it has established an oversight and enforcement mechanism using the Federal Privacy Commissioner and the Federal Court. Although PIPEDA encompasses most businesses, it is not applicable to government organizations — an important distinction.

A fundamental principle of PIPEDA is the required protection, both physical and technological, of personal information against loss or theft and safeguarding of that information against unauthorized access, use, modification, and disclosure. An additional aspect of the PIPEDA regulation is the ability of the individual linked to the collected information to not only find out what is being collected and managed but also to make corrections and changes to that information. Table 7 reviews the requirements of PIPEDA, IDC's best practices around ensuring organizational compliance, and the corresponding features in HP's IAM solution.

**TABLE 7****Identity Management Requirements of PIPEDA**

Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Absolute protection and privacy of data required; does not permit unauthorized collection, storage, or dissemination	Audit, tracking, and reporting system	Audit and reporting with real-time altering features
Ability for individuals to request a review of their stored data and make changes to it if so desired.	Password and profile management system	Password and profile management, personalized user experience, single sign-on support
Protection of stored data from unauthorized internal and external threats	Centralized identification and authorization system	Single sign-on, delegated administration
Need to report on compliance	Reporting system	Audit and reporting with real-time alerting

Source: IDC, 2005

**Gramm-Leach-Bliley Act of 1999 (GLBA)**

Also known as the Financial Services Modernization Act of 1999, GLBA provides limited protections for consumers against the sale of their personal and private financial information. Additionally, GLBA offers protections against individuals who would gather financial information on the basis of false pretenses. Concerns that brought about the adoption of this act stem from a similar source as those for HIPAA. GLBA originally intended to lift the ban on the ability of banks, brokerages, and insurance companies to merge. However, since that ban was lifted, these companies can gather significant personal finance and medical information on their customers.

Therefore, GLBA has established some rather weak methods of providing consumers the opportunity to protect their information. The first option, and most applicable to this paper, is that financial companies, brokerages, and insurance companies must protect sensitive data from potential threats as well as unauthorized access, use, or distribution. The second and third options require the aforementioned firms to provide consumers with copies of their policies and offer opt-out options for the internal sharing of some personal information. However, compared with similar acts in other geographies, GLBA is quite weak. Table 8 outlines the important regulation requirements of GLBA, IDC's best practices, and the corresponding features in HP's IAM solution.

**TABLE 8****Identity Management Requirements of GLBA**

Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Manage and track access to customers' private financial information	Centralized identification and authorization system	Single sign-on, automated user/resource discovery, audit and reporting with real-time alerting
Restrict access to customers' private financial information	Comprehensive workflow and user management system	Workflow, delegated administration, automated user/resource discovery
Provide reporting and proof of protection of data and compliance	Robust audit, tracking, and reporting system	Audit and reporting with real-time alerting

Source: IDC, 2005

**Directive 95/46/EC — European Union Privacy Act (EUPA)**

The full name of the European Union Privacy Act is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Several articles within the EUPA address the protection and security of personal data. The first part of the EUPA deals with the proper methods for collection, storage, and use of personal data. It requires that consent for use and collection be given by the subject to whom the data is attached. Several types of data, such as ethnic origin and political opinions, are prohibited from collection. As well as methods and data types, EUPA stipulates the rights of the subject to object to the collection as well as access and update their public information.

Article 17 of EUPA focuses on the data protection requirements for businesses. This article requires businesses controlling individuals' public data to provide measures to protect that data against accidental or unlawful loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Following in the footsteps of Article 17, Article 23 provides for the liability and responsibility of businesses collecting personal information to protect said information. Distinctly lacking from the EUPA are actual punitive measures. Instead, EUPA is worded so that each member state is responsible for setting up the penalties for transgressions.

Also important is Article 25, which disallows the transfer of personal information to any third country unless that country has data protection/privacy measures that meet the requirements of an "adequate level of protection." If that third country has inadequate measures of protection, then European Union member states are liable for preventing and required to prevent the transfer of data to that third country. Needless to say, this situation has caused some strife with the United States

because U.S. regulations do not yet stand up to the requirements of EUPA — thereby requiring the creation of the U.S. Safe Harbor agreement, which is causing its own set of complications. Table 9 summarizes the requirements of EUPA, IDC's best practices, and the corresponding features of HP's IAM solution.

**TABLE 9**

**Identity Management Requirements of EUPA**

Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Provide technological means to prevent unauthorized access, alteration, loss, or disclosure of personal data	Centralized identification and administration system	Single sign-on, delegated administration, workflow, automated user/resource discovery
Provide technological means to protect data from misuse, unauthorized transfer, or disclosure	Comprehensive workflow and user management system	Workflow, delegated administration, automated user/resource discovery, audit and reporting with real-time alerts
Restrict collection to certain types of data	Comprehensive workflow and alerting system	Workflow, audit, and reporting with real-time alerts
Obtain consent for collection of any personal/private information from the individual to whom the information is attached	User-friendly password and profile management system	Password and profile management, personal user experience, single sign-on
Disallow the transfer of information to any country with substandard data protection laws	Audit and alerting system	Audit and reporting with real-time alert, workflow, and administration

Source: IDC, 2005

**California Senate Bills 1386 and 1950**

California SB 1386, which went into effect in July 2003, requires that all businesses and state organizations that conduct business in California and own or license computerized data containing personal information disclose any breach to the security of personal data of a resident of California whose unencrypted information is, or is reasonably believed to have been, acquired by an unauthorized person.

This bill stipulates that if the data has been compromised, then the business or agency must provide notification to the individual through a variety of methods. Generally, notification should be in writing, either through the mail or through email. However, if such notification attempts are unsuccessful or if the information on the person is limited, then the business may fulfill its obligation through a public notification method, such as a posting on its Web site or other prominent location where the subject may be able to access the information.

In addition to SB 1386, SB 1950 expanded the requirements of businesses. That is, it requires that businesses that maintain records on California residents provide reasonable security measures and procedures to protect the personal and private information of those individuals. It also requires that if sensitive information is to be passed to a nonaffiliated third party, then the business must have a contract from the third party stipulating that it have protection in place to secure the personal and private data. SB 1950 also absolves certain businesses from this requirement, including medical and healthcare companies, financial institutions, some governmental organizations, and any company that is regulated by legislation with more restrictive requirements.

Table 10 identifies the regulatory requirements of California Senate Bills 1386 and 1950, IDC's best practices, and the corresponding features in HP's IAM solution.

<b>TABLE 10</b>		
Identity Management Requirements of CA SBs 1386 and 1950		
Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Prevent unauthorized access or disclosure	Centralized identification and authorization system	Single sign-on
Protect data from misuse and unauthorized access	Comprehensive workflow and user management system	Workflow, delegated administration, automated user/resource discovery
Alert individuals if information has been compromised	Reporting system	Audit and reporting system with real-time alerts, password and profile management

Source: IDC, 2005

### **Japanese Personal Information Protection Act 2003 (JPIPA)**

Submitted to the Japanese Diet in April 2001, passed in 2003, and completely enacted by April 1, 2005, JPIPA is aimed at protecting personal data and regulating the acquisition, custody, and use of personal information. The main issue with JPIPA was that journalists were among the individuals covered by the act — which the journalists vocally and energetically disputed.

Although most privacy regulations provide for a "freedom of the press" clause, JPIPA did not include such a clause in its initial stages. This omission created a rather significant uproar from the media community, which felt that it was a covert attempt by the government to censure the media. After significant deliberations and several failed attempts to pass before the Diet, JPIPA eventually addressed most of the requirements from its constituents and was passed in 2003. In summation, the act requires the following from businesses:

- Specify purpose for collecting and using personal information
- Do not collect information by fraudulent or unfair means
- Promptly notify the subject of the purpose for which his or her personal information will be used
- Ensure securing of personal data from loss and unauthorized access/disclosure
- Refrain from giving personal data to third parties without subject's consent
- Permit individuals to access and correct personal data

The complexity that surrounded JPIPA's creation continues to exist in its oversight. Four ministries are involved in the oversight of JPIPA: the Ministry of Economy, Trade, and Industry; the Ministry of Public Management, Home Affairs, Posts, and Telecommunications; the Ministry of Finance; and the Ministry of Health, Labor, and Welfare.

Ministers may require a business to report on its handling of personal information for the purpose of establishing whether or not the company is in compliance with the act. If a business is found to be in violation of the laws, then ministers may "recommend" that the business cease breaking the law and correct the problem. The act provides for small fines (up to 300,000 yen or US\$2,700) or up to six months in jail. Corporations may be liable separately under the act and held accountable for the actions of their representatives, agents, and employees.

Table 11 reviews the regulatory requirements of JPIPA, IDC's best practices, and the corresponding HP product features.

<b>TABLE 11</b>		
Identity Management Requirements of JPIPA		
Requirement	IDC Best Practice	HP IAM Solution Feature(s)
Promptly notify the subject of purpose for which personal information is being used	Reporting system	Audit and reporting with real-time alerts
Secure personal data from loss and unauthorized access/disclosure	Centralized identification and authorization system	Single sign-on
Restrict the distribution of personal information to third parties without the subject's consent	Workflow and user management system	Workflow, delegated administration, automated user/resource discovery
Provide individuals with the ability to access and correct personal data	Password and profile management system, user-friendly interface, user management system	Password and profile management, personalized user interface, automated user/resource discovery

Source: IDC, 2005

## CASE STUDIES

The following section of this white paper reviews a select number of case studies that show how enterprises can successfully use IAM solutions to address compliance and still achieve business benefits.

### Case # 1

A global transaction processor for banks, ATMs, EFTPOS, credit cards, and Web payments needed to provide extranet access to its corporate clients. The firm expected to have 400,000 users by mid-2004 and therefore required a system that would allow it to protect a range of distributed banking services. The company required assistance in solving its challenges and turned to HP for its solution.

Utilizing HP's service-oriented and federated identity management products, the firm not only met its planned rapid deployment and time-to-market goals but also achieved a lower-than-expected total cost of ownership (TCO) in doing so.

Utilizing HP's service-oriented and federated identity management products, the firm not only met its planned rapid deployment and time-to-market goals but also achieved a lower-than-expected total cost of ownership (TCO) in doing so.

### Case # 2

A large electronic funds transfer (EFT) clearinghouse owned by multiple banks must deal with the challenge of a federated membership of banks. The banks need to be able to securely track the status of and modifications to transactions online. Additionally, the member banks need to be integrated online with a standard framework for accessing the network.

In turning to HP, the clearinghouse utilized the following HP IAM features to help bring together its banks and realize its goals: service-oriented and federated identity management, delegated administration, identity-based personalization, and secured audit. Using these key IAM features to integrate the banks, the clearinghouse has recognized advantages such as increased time to market for member banks to federate their identity systems, near-real-time tracking of EFTs, better and feature-rich user interface, federation-based privacy controls, and a change management audit system. These options improve the clearinghouse's ability to keep up with the government privacy regulations.

### Case # 3

A very large international post-trade financial services company requires millions of daily transactions that may run in an average daily value of up to \$3 trillion. Given the complexity of the systems, audits required two weeks or longer to complete. The system includes more than 5,000 customer organizations, each with over 1,000 users and multiple tiers of business relationships (up to 5). It also includes over 30 customer-facing services, each of which has more than 3 resources, and the resources are administered by 8 different acquired business units using 20 different administration tools. The firm's goals were to reduce the complexity of its systems and comply with government privacy regulations while increasing the speed of doing business.

The firm chose HP's service-oriented identity management and audit and reporting tools. The combination of these tools provides real-time audits and audit information augmented and segmented by business services. Therefore, with the introduction of the new HP system, the firm was able to control and monitor user access to identity data, financial process, and business services. Also, it was able to provision identity services based on contextual business models; implement approvals-based change management and workflow; and deploy a tamper-resistant audit of all access requests, authorization decisions, and administrative changes/approvals. Using HP's secured audit and reporting tools, the firm can now demonstrate to regulators that it meets compliance regulations. Moreover, the firm's plan includes reporting based on specific regulations, and the reporting can also be extended to third-party products such as Oracle Financials and J.D. Edwards.

---

#### **Case # 4**

A large government agency in Europe supports an information exchange between two departments that provide social security and employment benefits to private citizens. The agency currently provides more than 18,000 public sector employees from multiple departments with access to citizens' records relative to employment benefits and welfare entitlements. Because of the sensitivity of the data, the law requires the agency to rigorously protect the privacy of the information it manages. The government decided to reorganize the employment and social security departments to allow citizens to more easily access their benefits, and thus the agency was mandated to find a system that would enable all the relevant public sector employees to strategically, yet privately, share data from their individual information databases.

The agency selected HP OpenView Select Access to provide the centralized authentication and authorization layer to the system, manage user access privileges according to centrally set policy, and delegate the administration of those privileges to the individual departmental units.

"We chose HP OpenView because we felt that Select Access was the only Web access security product with the right combination of ease of use, security, flexibility, and cost-effectiveness for the project. HP OpenView was selected as a partner on whose expertise and commitment to the global government sector we could rely to deliver this critical project. Over the last year, our decision has proved to be correct. User and policy management has been integrated into the business process of the different departments, usage has grown from 1,000 to over 18,000 registered users, and overall security has improved," said the general manager of infrastructure integration and remote services.

"We chose HP OpenView because we felt that Select Access was the only Web access security product with the right combination of ease of use, security, flexibility, and cost-effectiveness for the project," said the general manager of infrastructure integration and remote services.

The result of the partnership between the agency and the integrator was a solution that became the "one-stop shopping" service that the government needed. Unemployed citizens are able to go to one place to look for new employment and investigate other benefits. The new environment boasted strategic data sharing while protecting the personal information of the citizens through robust centralized policy — just what the organization needed to ensure compliance with governmental regulations.

## **CONCLUSION**

As sensitive information and data continue to be collected and gathered, governments will increasingly find ways to constrain and hold accountable the enterprises that are doing the collection to ensure that the data remains accurate, private, and protected. Important components of complying with these regulations are the managing and monitoring of access to data protected under such regulations.

Compliance, however, shouldn't be the end game. Organizations should look for the business benefits that can come with deploying a new system, such as an identity management solution, to comply with regulations.

IDC suggests that an IAM system, such as HP's identity management solution, can be used in conjunction with intelligently developed policies and processes to help enterprises achieve the compliance required by regulations and simultaneously fulfill the need for increased business benefit and value.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2005 IDC. Reproduction without written permission is completely forbidden.