

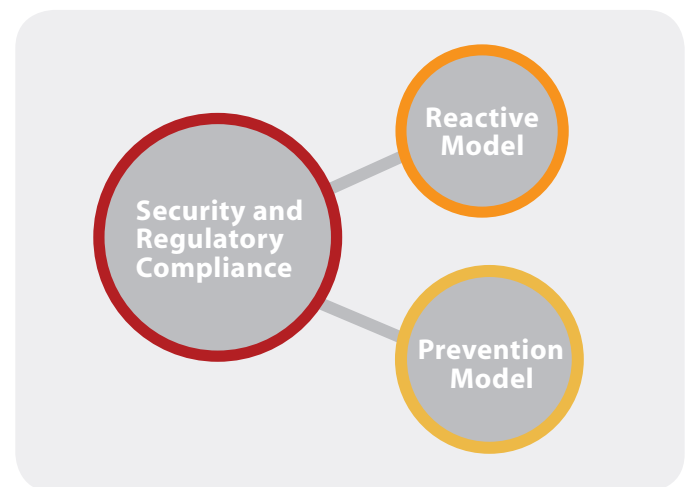
Organizations of all sizes continue to struggle with increasingly complex audit regimes that are driven by compliance requirements. This is particularly true of companies in the financial, health care, and professional services industries such as law and accounting that must comply with myriad conflict of interest regulations directly affecting how they manage electronic communication between different functional areas of their organizations. These barriers can be created and enforced in a variety of ways and are often referred to as “Information Walls”. This paper will detail the pros and cons of two different approaches to enforcing the concept of information walls as well as provide an overview of a system designed to implement information walls in a variety of regulated environments.

The system of internal controls around compliance management for information walls is much the same as it would be in other auditable areas. It requires separation of duties, access limitations, review processes and proper documentation; among others. As such, the internal audit team should initially consider whether the information controls are **manual** or **automated**.

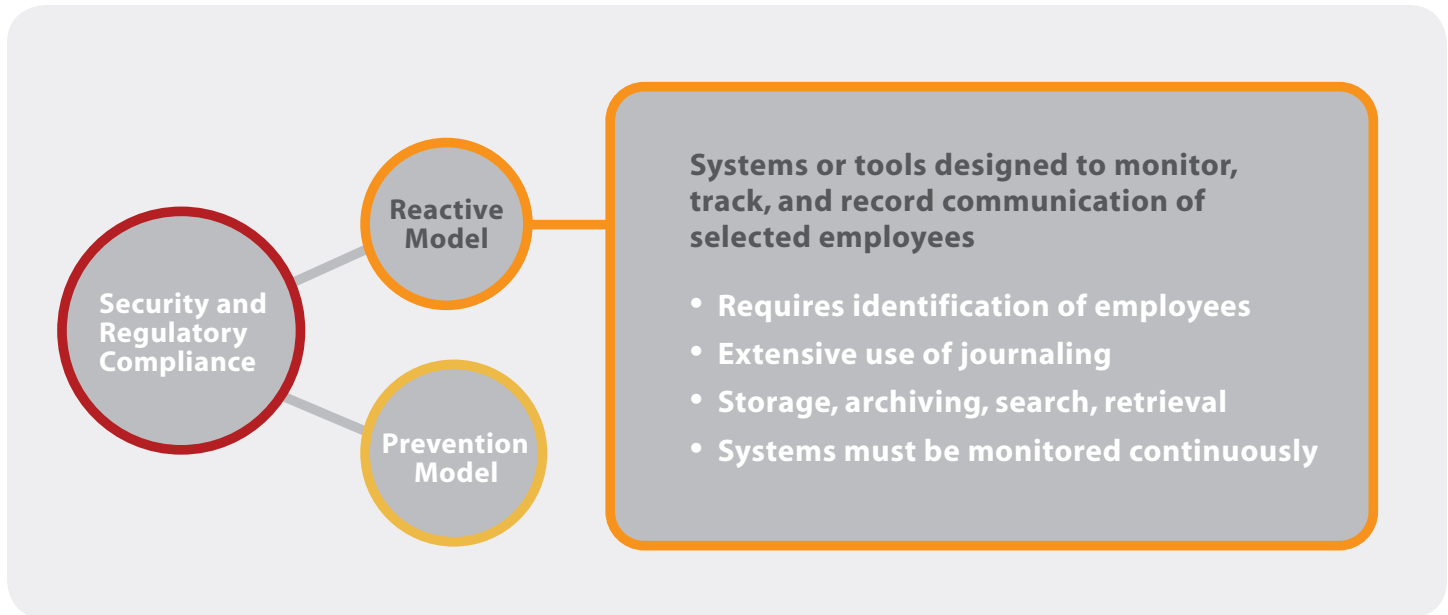
For the purpose of this discussion we will focus on technology designed to automate these processes. Manual controls are more prone to errors, difficult to track, and are harder to enforce from an audit perspective. Where technology does support the compliance effort—and this is certainly a growing trend—internal auditors need to confirm that compliance personnel understand the technology and are involved in the decisions to purchase, implement, and modify it.

Generally speaking, it’s important to keep in mind that there are two types of compliance automation related to information walls:

- ▮ **Reactive Model**
- ▮ **Prevention Model**



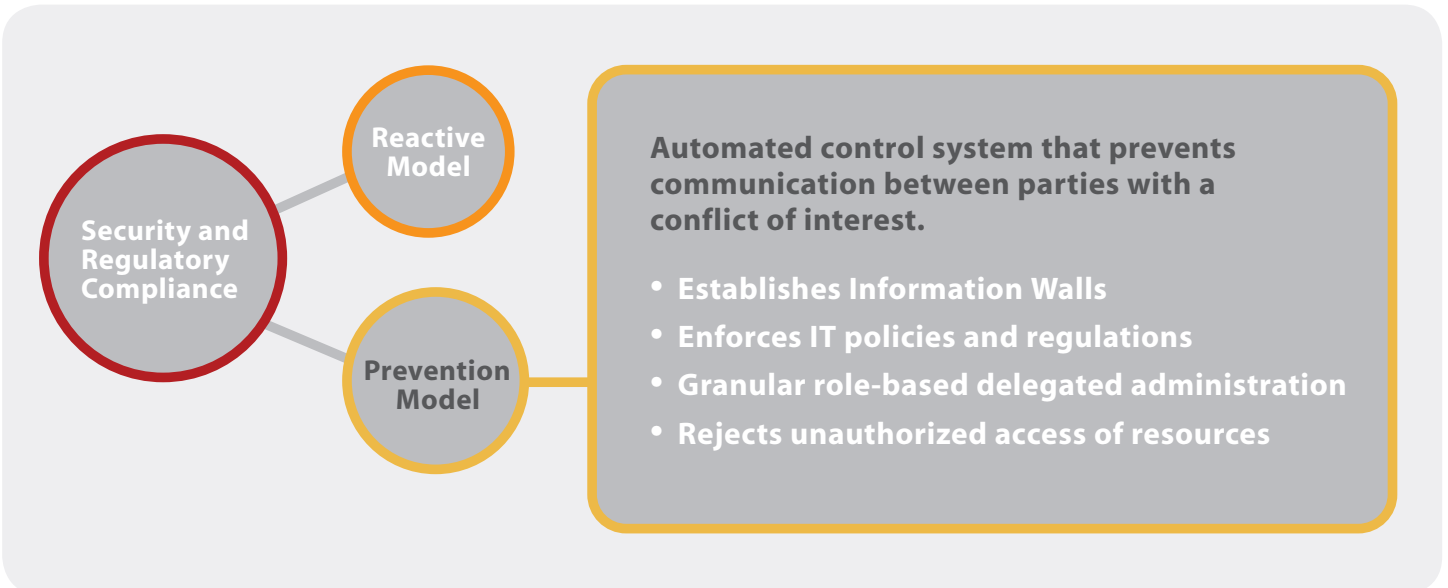
### Reactive Model



The reactive approach requires “regulated” employees to be identified and their communication tracked, recorded, and archived. Traditionally, this approach has relied primarily on journaling of all electronic communication – trapping every keystroke – and then archiving that communication for future reference. In the event of a dispute, investigation, or audit, recent information as well as archives must be navigated and searched for specific content. Once found, it must be reproduced, including communication via distribution lists. During an audit, it must be demonstrated

that all communication is searchable, can be tracked, archived, and is reproducible on demand. This can be a daunting task given the mobility and volume of electronic communication. Similarly, searching the email and archival databases and then reproducing specific communication from those sources is complex and time consuming. Once identified, the communication must be analyzed to determine if it has violated an established policy or rule. This is obviously much more complex in situations involving litigation.

### Prevention Model



The prevention model provides the ability to enforce “information walls” by simply preventing electronic communication between parties with conflicts of interest, such as energy traders and energy producers or equity traders and mergers-and-acquisition professionals. The implementation of a prevention model revolves around regulations or internal security models designed to force businesses to implement and enforce information barriers between these various groups. These information barriers are typically implemented to restrict access to certain entities and objects based on rules defined by the organization or mandated by the governance controls. While most of the time these rules are static and based on pre-defined constraints, there are certain

conflict of interest classes that mandate dynamic adaptation by the information barriers.

Consider an example where access to research and client information in a consulting firm is controlled by a dynamically changing information wall. By default a consultant has access to all research and client information. However as soon as the consultant has read a document on say insurance firm A, access to all documents related to insurance firms other than A is revoked. This is done to avoid possible conflicts of interest and decisions based on confidential information about the competitors of insurance firm A, who may also be clients of the consulting firm. The information barrier is dynamically adapting to changing constraints

as users are accessing various resources in the system.

The advantage of this approach is clear - there can be no communication between the specified, regulated entities. The audit process is simplified because it requires a review of the logic used to determine where conflicts of interest occur. This limits much of the complexity and expenses associated with the reactive approach that relies on journaling and archiving systems.

### Solution Review – Ensim Unify Distribution Group Manager

It should be clear that the two models employ very different technical systems to enforce compliance policies and facilitate regulatory audits. The **reactive model** commonly relies on log files or journaling to detect modifications and record data with respect to all regulated actions. Individual client applications or program agents might be required that attach to systems (for example, directory, databases, email servers etc.) through the application's API and provide monitoring and reporting services. Compliance reports are created that detail breaches and their responses. Under this scenario, a regulatory

audit requires retrieving log and journal archives, searching and reviewing the logs and filtering out regulated actions.

An example of a reactive system would have a database to store and archive all the journal information, multiple program agents running on the systems to intercept data, and a reporting system to search and present the information to compliance officers. On the other hand, the implementation of a **prevention system** revolves around regulations or internal security models designed to allow businesses to implement and enforce information barriers. These information barriers are typically implemented to restrict access to certain entities, objects, resources or networks based on rules defined by the organization or mandated by the governance controls. While most of the time these rules are static, based on pre-defined constraints, there are certain conflict of interest classes that mandate dynamic adaptation by the information barriers.

This model simplifies the audit process because it requires only a review of the logic used to determine where conflicts of interest occur.

This limits much of the complexity and expenses associated with the reactive approach

## The Compliance Perspective

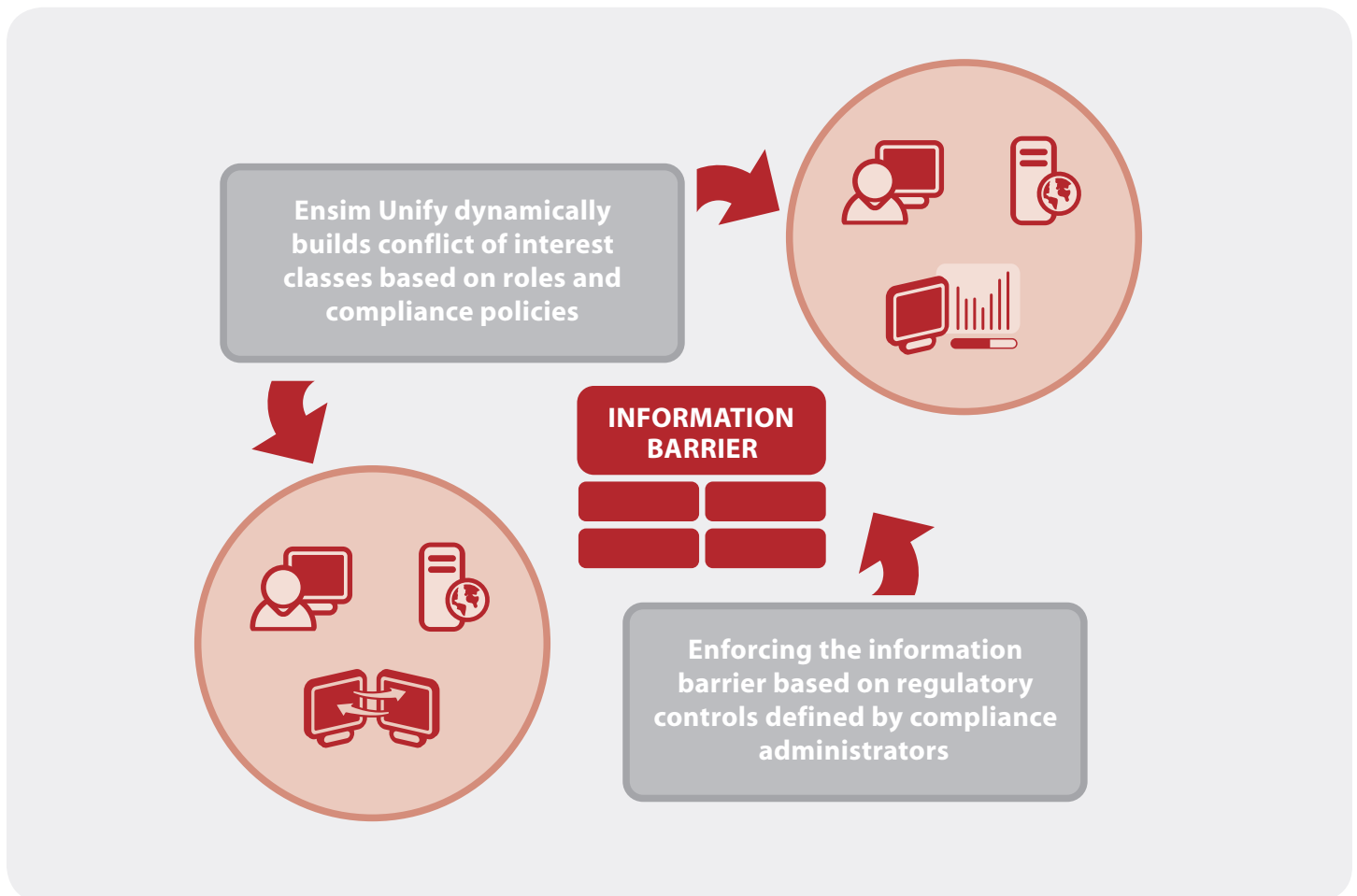
that relies on journaling and archiving systems and the ability to extract specific information.

It should be clear at this point that a properly designed prevention model would be a much more efficient and accurate way of enforcing compliance. Here is an example of how a typical prevention system will work:

The two circles in this diagram below represent two different conflict of interest classes that are separated by an information barrier

regulating resource access or information exchange between these groups. Each of these classes represents Distribution Groups in your Active Directory. Each class relies on either a static compliance definition or dynamically adapting constraint based on your conflict of interest policies.

The information barrier created between the two DGs is periodically updated based on the current membership of the two conflict classes.



## The Compliance Perspective

Referring back to our consulting company example, the information system would create two DGs representing the two conflict of interest classes. The first one will include all the resources related to the Insurance Company A project. The second one includes documents and resources associated with all other insurance companies. Once these group definitions are defined in the databases, the system will construct this information barrier restricting all communication or resource access between these two conflict classes or distribution groups. This would mean setting up mail routing to prevent email communication, updating phone systems to drop phone communication, and setting up permissions to prevent unauthorized access. The advantages of this model are that system administrators do not have to explicitly manage access to entities or resources by

granting or revoking privileges. Instead, it is enforced by defining rules for each of the DGs and then having the compliance system automatically setup access controls and permissions to enforce these rules. The conflict of interest class definitions are stored in the Ensim Unify databases. With this approach, a proactive monitoring system is constantly monitoring various entities to make sure that all access control permissions are always up-to-date. This model is fast gaining popularity and is being adopted by leading financial institutions to enforce regulatory requirements designed to eliminate potential conflicts of interest.

### About Ensim Corporation

Founded in 1998, Ensim Corporation is the leading provider of compliance based solutions for user provisioning and access management. Ensim products are used by service providers and enterprises worldwide to accelerate and enable deployment of integrated solutions, simplify and automate secure management of complex environments, and increase user and IT productivity. Ensim is Microsoft Gold Certified. For more information, visit [www.ensim.com](http://www.ensim.com) or contact Ensim at 1-877-693-6746 or 1-408-496-3700 outside the United States.

Ensim and the Ensim logo are registered trademarks of Ensim. All trademarks or registered trademarks contained herein are the property of their respective owners.

