

## Audit and Compliance

Comprehensive visibility into the location, use and distribution of material, nonpublic private, and personally identifiable information in documents to understand the risks across your enterprise



### OVERVIEW

A myriad of privacy regulations across the financial services industry require companies to properly govern the use and distribution of information considered material nonpublic. However, auditing for compliance is difficult, since so much unstructured data resides across electronic documents, such as emails, spreadsheets, and word processing files. Adequately meeting this challenge requires:

- Knowing the location of all material information
- Knowing who has rights to access the information
- Knowing who has used or distributed the information
- Attesting to controls over the information, and
- Consolidating reports for all systems that store the information.

It is unrealistic to believe that these requirements can be met and results presented in a timely manner if relying upon manual efforts. An incomplete understanding of the information landscape, coupled with inability to track information use and distribution activities, creates insurmountable barriers to success and uncertain audits.

### THE SOLUTION

Companies can now solve these challenges by identifying unstructured material information and monitoring all access, use and distribution activities. The Audit and Compliance Solution provides distributed inventory and monitoring components that act as the basis for exceptional audit and compliance capabilities. The Solution's three primary components are:

#### Inventory

Provides the "what, where and who" aspects for material information. Identifying the material information, its location, and the rights associated with its use provides the basis for further data gathering efforts. The raw data can also be used to generate reports for audit and compliance.

#### Entitlements Audit

Inspects, aggregates and analyzes rights data for material information, and integrates this data with business practices data, to synthesize assessments of proper and improper grants of rights. Data can be used to expose outlier rights grants, rogue accounts, and rights attestation reports.

#### Activity Audit and Compliance Monitoring

Provides run-time introspection of the material information lifecycle. Through observation and documentation of all use and distribution activities related to material information, improper actions can be noted and acted upon proactively, eliminating unexpected results during audits.

### SOLUTION HIGHLIGHTS

- **Monitor for compliance** Understand who is accessing and distributing information that is governed by regulations
- **Streamline compliance audits** Provide auditors with attestations of proper entitlements and proof of controls over regulated information
- **improve analysis** Combine an understanding of what is happening to information with the knowledge of what risks can happen
- **Improve reporting** Provide reports grouped by regulatory mandates to management and auditors
- **Close gaps in compliance posture** Provide basis for gap analysis with activity monitoring and automated intervention that provides measurable controls

The Solution delivers unparalleled knowledge and controls for unstructured material information. The data gathered and presented by the Solution, and the additional controls, provide financial institutions with improved audit and compliance postures; but more importantly, the Solution greatly reduces the chance that material information will be improperly used or distributed.

## MATERIAL INFORMATION INVENTORY

- What documents must be protected from abuse
- What documents must be protected from unintentional distribution
- What centralized repositories contain material documents
- What distributed systems contain material documents, and
- Ownership of material document

## THE ENTITLEMENTS AUDIT

Builds upon the data gathered during inventory and gathers more critical data to gain key insights into data repositories to know:

- Who has access to what material documents
- What groups are defined for each repository
- Is group membership consistent across repositories
- What groups have access to what material documents, and
- What entitlements are set across every shared resource

## COMPLIANCE MONITORING

Run-time functionality about the use and distribution of material information. By implementing activity audit and compliance monitoring, companies benefit from an understanding of what is happening to their material information, complementing their understanding of what can happen provided by inventory and entitlements audit. The company will know:

- When any material information is accessed
- Who accesses specific information
- Who modifies it
- When information is distributed
- Who distributed it
- To whom was it distributed, and
- What information is distributed

## REPORTING FOR COMPLIANCE

Packages the reporting capabilities provided by the Solution for specific regulatory compliance scenarios, such as:

- Gramm-Leach-Bliley Compliance
- Sarbanes-Oxley Compliance

An example is provided below. Other packages and scenarios are possible by using the Solution; contact NextLabs for more information.

## NEXTLABS

© 2007-2016 NEXTLABS INC. ALL RIGHTS RESERVED

## GRAMM-LEACH-BLILEY COMPLIANCE EXAMPLE

Non-public Personal Information Protection Scenario:

- List all documents containing nonpublic personal information (NPI), sorted by repository
- List all users entitled to access each listed repository
- Provide attestation reports for information owners, managers
- List all accesses to NPI during current month, current quarter
- List all accesses to NPI during previous quarter
- List all duplication of NPI during current quarter and sorted by user

## SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs implements the Solution by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, as well as defining information control policies.

### Step 1: Requirements Gathering

NextLabs works with you to understand your infrastructure, and security & policy requirements.

### Step 2: Risk Assessment

We help you discover and identify current risks to help prioritize solution requirements with clear visibility into your environment.

### Step 3: Policy Configuration

Audit & compliance policies are designed and electronically codified.

### Step 4: Install Policy Enforcers

Policy Enforcers are deployed across applications and systems to gather data, when applicable to the requirements.

### Step 5: Knowledge Transfer

Finally, NextLabs helps train your team to maintain the Solution.

## ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit <http://www.nextlabs.com>.