



# Financial Services

**Information Risk Management Solutions to Automate Audit & Compliance, Centralize Entitlements Management, Enforce Information Barriers across Communication Channels, and Prevent Data Loss**



## Information Risk Management Challenges

Financial services companies are under intense scrutiny due to high-profile cases of improper data disclosure, including analyst research shared with bankers, client deals disclosed between internal teams, and confidential client data misdirected via e-mail to unauthorized recipients. Moreover, the inability to centrally manage a consistent set of policies across data to control unauthorized access and use, and a lack of comprehensive auditing, has led to increasing risk exposure.

SEC, NASD and NYSE regulations, BSA, and Sarbanes-Oxley rules, require strict enforcement of boundaries to preserve data confidentiality. GLBA, CA SB 1386, and similar mandates also require personally identifiable information (PII) to be kept private. With non-compliance penalties and loss of revenue including regulatory fines, legal liability from clients and shareholders, and loss of brand value, financial services organizations must actively control the loss of material nonpublic data to limit risks.

Unfortunately, today's silo solutions and system-specific controls do little to protect data once exported from repositories, nor do access controls understand the context of how data should be handled and disclosed properly across complex organizations. Gaining comprehensive visibility into data loss, and automating and maintaining a single set of top-down policies that maintain information confidentiality, are essential to improve compliance and mitigate risks.

## The Solution

The Solution includes key applications for material nonpublic information audit and compliance, conflict and disclosure management, centralized entitlements management, and enforcement of controls to prevent data loss and conflicts of interest. Financial services companies can now comply with industry regulations, mitigate data loss and unauthorized access, and simplify audit by centrally managing information use activities, implementing entitlements—and putting in place information barriers, document handling workflow, and disclosure policies—for material nonpublic information.

### ***Identity-Driven Policy to Enforce Data Confidentiality and Data Protection Controls***

The Solution addresses requirements for the discovery, access control, handling and protection of data. It integrates with and leverages existing infrastructure to apply identity-driven policies across users and resources. Identity-driven policies understand user context and environment variables during enforcement. Financial services companies can:

- Identify material nonpublic information
- Centrally define authorized users and proper entitlements
- Control data access, use, disclosure, and information barriers across the enterprise
- Align controls with corresponding business policies, regulatory rules, and contractual obligations, and

## Financial Services Applications

- **Audit & Compliance**  
Discover and classify unstructured data to identify access and usage risks
- **Enterprise Entitlements Management**  
Centrally configure, administer, enforce, review, and audit fine-grained access policies and authorizations to mitigate unauthorized access, simplify audit, and improve compliance
- **Information Barriers**  
Protect communication and collaboration to prevent conflicts of interest and avoid regulatory violations
- **Data Loss Prevention**  
Stop leakage and improper data loss, inside and outside the enterprise



- Provide a full audit trail of data flow history and user activity to satisfy internal and regulatory compliance requirements.

## Key Applications

The Solution includes four (4) key applications to address information risk management problems and workflow scenarios that are specific to financial services companies.

### Audit and Compliance

Gain visibility and understanding of the location, access rights, use, and distribution of material nonpublic information. Reporting and analytical capabilities provide:

- **Inventory details** – centrally aggregates information on “what, where and who” by identifying material nonpublic information, its location, and the rights associated with its use
- **Entitlement audits** – reports and audits access rights for material nonpublic information, and analyzes if access rights are properly granted
- **Activity audits and compliance monitoring** – provides run-time introspection of user activity throughout the material nonpublic information lifecycle.

Ease audits, improve compliance, accelerate conflict and disclosure analysis, and proactively implement information compliance.

### Enterprise Entitlements Management

Centrally configure, administer, enforce, review, and audit fine-grained access policies and authorizations. Standardizes the management of entitlements

across unstructured data repositories to reduce the cost of administration; simplify the audit of authorizations for compliance; and enable IT to implement fine-grained access control across applications quickly to react to business change, regulations, or legal inquiry.

### Information Barriers

Comply with industry regulations by auditing and enforcing boundaries during communications and collaboration. Identity-driven policies prevent information sharing between groups of users by requiring the proper use of confidential data to avoid violations.

### Data Loss Prevention

Information on desktops or mobile devices is easily leaked when copied to removable media, uploaded or copied to unsafe areas such as unsecured FTP, or misdirected via e-mail or IM to wrong recipients. It is important to protect material nonpublic data and applications from inappropriate access and use, even when users are off the network or disconnected, while educating them of policies, and automating document workflow and remediation procedures to eliminate user errors and simplify use.

## Solution Deployment

NextLabs utilizes a combination of GRC and security expertise, industry best practices, and proven services and implementation methodology to deliver a solution built on its leading information risk management software. The deployment process includes:

- **Step 1:** Monitor, record, and analyze information handling activities to discover and identify the risks of data loss.
- **Step 2:** Author, manage, and deploy policies using a XACML-

based 4GL policy language (ACPL®) to achieve information compliance and data protection controls across applications and communication channels.

- **Step 3:** Apply controls to educate users about policies and procedures; automate workflow and remediation to improve data handling; or block activities or alert policy stakeholders.
- **Step 4:** Measure the effectiveness of information compliance and protection controls with reporting, continuous audit, and compliance analysis.

## About NextLabs

NextLabs®, Inc. is the leading provider of policy-driven information risk management software for Global 5000 enterprises. Our software offers a cohesive solution for improving compliance and mitigating information risk by preventing internal and external data loss, eliminating conflict-of-interest activity, and ensuring proper access to applications and data.

Our flagship products, Enterprise DLP™ and Compliant Enterprise®, combine identity-driven policy with fine-grained access control and data loss prevention technology to protect data and enforce entitlements. By reducing the risk of data loss and unauthorized access to applications and data, NextLabs helps organizations ensure public confidence, demonstrate compliance, and maintain competitive advantage.

**For More Information, Visit  
www.nextlabs.com or Call  
800-898-3065**