



Risk Assessment Program For Information Barriers

This Risk Assessment Program provides a valuable service that helps identify your user and information activities that are subject to conflict of interest risk. The program will help your company start to identify information access and usage patterns, apply proper access controls, and prevent conflict of interest violations.

Information Risk Management

Reducing information misuse and improper disclosure is a major concern for today's enterprise. Monitoring and controlling information entitlement rights to identify and mitigate risk is an imperative for data security and compliance. Rapid, dynamic implementation of information control procedures is essential to remain competitive. Now, businesses are more exposed due to increased connectivity, workforce mobility, and dependence on global supply chains consisting of remote users, partners, outsourcers, and suppliers.

Managing information risk, achieving compliance with industry regulations such as, SEC, NASD and NYSE rules, and protecting data from conflict of interest violations are challenging within dynamic, complex information networks. Protecting data, training workers to act responsibly, and demonstrating control of information can be costly and time-consuming. Business leaders strive not only to meet compliance and control risk, but also to achieve greater effectiveness and productivity.

Why is Managing My Information Risks Difficult?

Managing conflict of interest risk begins with a factual assessment of where sensitive data is; how it is being accessed; what conditions are creating risk. Yet discovering and identifying this baseline data, especially during the time access is attempted, can be extremely difficult.

For example, client documents can be stored on central file servers and Microsoft® SharePoint® with access granted from the bottom-up to all account teams, regardless of considering client competing interests. Or confidential research can be shared with sales teams by analysts prior to publishing by using removable media, or email or IM.

To avoid conflicts of interest, businesses must consider real-time conditions to evaluate and ensure proper information disclosure. Factors during access and use, such as file metadata attributes; user or group role; locations of data, user, or connecting devices; time of access or use; and similar conditions can determine risk exposure level.

The Information Risk Assessment Program

The program addresses the difficulties associated with discovering and identifying information access and use activities. This insight is necessary to help you develop and strengthen your efforts in managing conflict of interest risk and regulatory compliance. You can learn who currently owns or has access to sensitive data, how to ensure proper information control policy, and where conflict of interest activities are occurring.

What Does the Program Do?

You are provided a "snapshot" of user and information activities. This includes the access and handling of sensitive information, inside and outside your organization, on or off your network. You will receive baseline data that helps you discover the level of risk of improper information access and handling, and conflicts of interest. You can uncover deficiencies or gaps in current security practices to improve and automate compliance and audits. Our findings and recommendations will help you:

- **Educate users on proper ways to access and handle sensitive or proprietary data:** Discover areas to focus or improve policy training. Improved education helps users to access and handle information in a manner that is compliant with your policies.
- **Automate information security rules and information access and handling procedures:** Obtain insight into the volume and types of sensitive, confidential data or intellectual property that are vulnerable to conflict of interest violations on your corporate network. Automating procedures can improve efficiency, and reduce complexity and errors.
- **Identify or discover policy gaps:** Gain awareness into potential non-compliance due to unintentionally risky or undefined procedures. Such gaps may include data stored to public directories or user access rights assigned improperly. Simplifying or optimizing security rules or procedures can close these gaps, and improve policy effectiveness and manageability.

What Will I Receive from the Program?

You will receive concise facts focused at user and information access and handling activities at data servers, portals, and endpoints (e.g., Windows file servers, Microsoft® SharePoint, Linux file servers, Windows PCs and laptops), along with our analysis and recommendations.

Our discoveries, analysis, and recommendations are delivered in a presentation and *Executive Conflict of Interest Assessment Report*. The report provides a view into:

■ **Information Barrier Violation Risk:** File access, use and sharing by user, time of access, access location by user or data, and proportion of access outside business hours and remote access. Information activities that may indicate conflicts of interest include:

- What information is exchanged between groups.
- How often is information exchanged between research and investment teams, departments, etc.
- What data is sent between groups over email or IM.
- What is the frequency of information sent to an unauthorized group (e.g., a customer document sent to another, unauthorized, customer).
- How is customer information handled by account teams that support multiple customers?

■ **Overprivileged Users:** Many IT organizations grant access privileges to more users than required, creating unknown conflicts of interest. This report details:

- Which authorized users and groups have access rights, but have *not* accessed information on file servers or SharePoint servers.

Report findings can then be used to limit access only to appropriate users with rights to sensitive data.

■ **Control Point Summary:** Information activities summary for specific applications, endpoints, or information repositories (e.g., client file server, SharePoint, laptops, Outlook clients). Activities can include:

- What confidential files were attempted to be accessed on a system or shared using an application.
- What data is accessed or shared based on group role.
- Which users have accessed or shared specific files.
- What information is accessed or shared most.
- Which users access or share the most information.

Our findings will identify areas of risk and recommendations for rapid remediation when necessary.

How Do We Engage?

The program engagement process is designed to be convenient for you and transparent for your organization, making it easy to achieve fast results. Minimal client-side software installation is needed in your user environment.

Once you contact us, one of our Information Risk Professionals will respond to answer your questions and provide you with a questionnaire:

1. You complete a simple questionnaire that we provide.
2. Using the information you provided in the questionnaire, we will conduct a brief discovery session with you to establish success criteria for the assessment exercise. This will include, as applicable:
 - a. Identify a set of sensitive information locations, sites, and applications. We may need an LDIF export from Microsoft® Active Directory®.
 - b. Identify a set of applications, endpoints, and servers that you will conduct the information barrier assessment upon. We may need access where an agent can be automatically installed.
3. We will quickly configure and deploy the necessary software to perform the discovery. User and information activity data will be collected unobtrusively, based upon the requirements you have provided.
4. After a period of data collection, we will synthesize and provide you with the results and our analysis in a Risk Assessment presentation and *Executive Conflict of Interest Assessment Report*.

Time Requirements: Depending on the computing environment and success criteria, the program can take as little as one week.

Confidentiality and Privacy Assured

All data collected is aggregated at our servers, hosted at a secured facility. All information and results from our analysis are held in strictest confidence and removed from our systems, post-engagement.

Get Started by Contacting NextLabs

For More Information about our Risk Assessment Program for Business Information Barriers:

- Call NextLabs today at **650-577-9101**
- Visit us on the Web at **www.nextlabs.com**