



Information Risk Assessment Program for Intellectual Property Protection

This Risk Assessment Program provides a valuable service that helps identify your user and information activities that are subject to IP leakage and conflict of interest risk. The program will help your company start to identify information access and use patterns, apply proper controls on IP, and prevent policy 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 and best practices, and protecting intellectual property data from leakage and conflict of interest violations are challenging within dynamic, complex information networks. Protecting IP, 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 data leakage and 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, software source code can be stored on central servers with access granted to an entire engineering team, regardless of competing product uses or conflicting client interests. Similarly, product designs and CAD files, downloaded from PDM, can easily be copied to USB removable media, or communicated over email or IM, where it is disclosed improperly within a supply chain.

To avoid risks, policies must be able to evaluate the real-time business conditions during IP access and handling. Factors 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 exposure.

The Information Risk Assessment Program

The program addresses the difficulties associated with discovering and identifying intellectual property access and use activities. This insight is necessary to help you develop and strengthen your efforts in managing IP leakage and conflicts of interest. You can learn who currently owns or has access to sensitive data, how to ensure proper information control policy, and where IP leakage or 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 intellectual property, 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 that can result in leakage or 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 intellectual property data:** Discover areas to focus or improve policy training. Improved education helps users to access and handle IP in a manner that is compliant with your policies.
- **Automate information security rules, and IP access and handling procedures:** Obtain insight into the volume and types of intellectual property, or sensitive, confidential data, that are vulnerable to leakage or 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 IP disclosed, 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 an *Executive IP Risk Assessment Report*. The report provides an extensive view containing:

■ **Information Access, Use and Disclosure Patterns:**

IP access and handling by user, time of access and use, access location by user or data, and proportion of access and use outside business hours, and remote access and use. Information activities can include:

- When and how different users, groups, departments, or organizations share intellectual property.
- Which users or groups access or use IP disproportionately outside of normal work hours.
- What information is accessed or used by users or systems that are outside of internal domains.
- What data is communicated to points outside the network or copied to removable media (e.g., USB).
- What systems are used to share IP.

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

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

Report findings can then be used to limit access only to appropriate users with rights to access or use IP.

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

- What intellectual property was attempted to be accessed on a system or shared using an application.
- What IP is accessed or shared based on group role.
- Which users have accessed or shared specific files.
- What IP is accessed or shared most.
- Which users access or share the most IP.

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 intellectual property 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 IP risk 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 IP Risk 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 that is 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**