



# Risk Assessment Program For Information Entitlements

**The Risk Assessment Program for Information Entitlements is a valuable service that helps identify your user and information activities that are subject to risk. This 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, and protecting data have become 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 information entitlement risks 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, if users attempt to access confidential data on a central server or Microsoft® SharePoint® server, it is difficult to control under what business circumstances information is allowed to be safely accessed, how it can be exported or saved, and where it can be safely stored. Entitlements must include real-time business dynamics to ensure proper access rights. Factors such as file metadata attributes; user or group role; data, library, or connecting device locations, time of access; and other conditions can determine risk exposure. For instance, a contractor who attempts to export intellectual property from a SharePoint engineering team design library, during non-business hours, to an unknown device located outside the network, may indicate an increased risk of improper disclosure.

## The Information Risk Assessment Program

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

### What Does the Program Do?

You are provided a "snapshot" of user and information access activities. This includes the access 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 disclosure, and conflicts of interest. You can uncover deficiencies or gaps in current security practices to improve and automate access control compliance and audits. Our findings and recommendations will help you:

- **Educate users on proper ways to access sensitive or proprietary data:** Discover areas to focus or improve policy training. Improved education helps users access information, internally or externally, on or off your network, in a manner that is compliant with your policies.
- **Automate information security rules and information access procedures:** Obtain insight into the volume and types of sensitive, confidential information or intellectual property that are vulnerable to leaking off your corporate servers. 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 information stored to public directories, or user information access privileges that are not properly assigned. Simplifying or optimizing information 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 activities at data servers and portals (e.g., Windows file servers, Microsoft® SharePoint, Linux file servers), along with our analysis and recommendations.

Our discoveries, analysis, and recommendations are delivered in a presentation and an *Executive Risk Assessment Report*. The report provides an extensive view containing:

- **Information Access Patterns:** File access by user, time of access, access location by user or data, and proportion of access outside business hours and remote access. Information activities can include:
  - When and how different users, groups, departments, or organizations access information.
  - Which users or groups access information disproportionately outside of normal business hours.
  - What information is accessed by users or systems that are outside of internal domains.
  - What systems are used to access sensitive data.
- **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 information on file servers or SharePoint.

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

- **Access Point Summary:** Information activities summary for specific information repositories (e.g., file server or SharePoint server). Activities can include:
  - What files were attempted to be accessed by any non-owner of that data.
  - What information is accessed based on group role.
  - Which users have accessed specific files.
  - What information is accessed most.
  - Which users access 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. No 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 servers that you will conduct the information entitlement assessment upon. We may need access where a server 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 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 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

Help your organization reduce information risks through our discovery and identification program.

Call NextLabs today at **650-577-9101** or visit us at **[www.nextlabs.com](http://www.nextlabs.com)** to take advantage of our Risk Assessment Program for Information Entitlements.