



Information Risk Assessment Program For Endpoints

The Information Risk Assessment Program for Endpoints is a valuable service that helps identify the kinds of user and information activities that are subject to risk. The service will help your company start controlling risk and integrity of information, or evaluate effectiveness of information handling and risk management strategies.

Information Risk Management

Reducing information misuse and improper disclosure is a major concern for today's enterprise. Monitoring and controlling information handling to identify and mitigate risks 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 risks begins with a factual assessment of where sensitive information is; how it is being used; how it is being shared. Yet discovering and identifying this baseline data, especially at computing endpoints, can be extremely difficult.

For example, when users copy confidential data from a central server or Microsoft® SharePoint® portal server to their local PCs, it becomes difficult to maintain control over who accesses it, how it circulates, how it is used, and where it is stored. Once they have a local copy, users can re-copy data to USB drives or CDs, attach or paste it into email or IMs, post it to collaboration portals with unknown access permissions, or simply move it to uncontrolled areas on or off the network.

The Information Risk Assessment Program

The Information Risk Assessment Program for Endpoints addresses the difficulties associated with discovering and identifying activities and information use data that is necessary to help you develop and strengthen your efforts in managing risk and compliance.

What Does the Program Do?

This program provides a "snapshot" of your organization's user and information activities. This includes the use and sharing of sensitive information inside and outside your organization, on or off your corporate network.

With this program, you will receive baseline data that helps you discover the level of risk of inappropriate information disclosure, and uncover any deficiencies or gaps in your current information security practices. Our findings and recommendations will help you:

- **Educate users on proper ways to handle sensitive or proprietary data:** Discover areas to focus or improve policy training. Improved education can help users distribute and share information, internally or externally, on or off your network, in a manner compliant with your policies.
- **Automate information security rules and information handling procedures:** Obtain insight into the volume and types of sensitive, confidential information or intellectual property that are vulnerable to leaking off your corporate desktops. 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 activities at computing endpoints (e.g. desktops, laptops), along with our analysis and recommendations.

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

- **External Bound Information:** Frequency of files sent through FTP, email, instant messaging (IM), or web-mail, grouped by originating user or group.
- **Access and Usage Patterns:** File access by user, time of access, application used for access, proportion of access outside business hours, and file usage.
- **Information Handling:** Proper or improper exercise of corporate information handling policies. Information activities can include:
 - Copying sensitive information to insufficiently secure folders/servers.
 - Exporting of data from applications or downloading of data from secure servers.
 - Deleting or modifying specific files against corporate records retention policies.
 - Sending unencrypted attachments in e-mail or copying to external drives, e.g. a USB drive.
 - Exporting data from ERP servers to insufficiently secure locations.
 - Saving sensitive corporate reports/customer data on local drive.

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

How Do We Engage?

The engagement process for this service is designed to be convenient. 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 which we provide to you.
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 users and desktops for data collection. We may need access to desktops where a desktop agent can be automatically installed.
3. We will quickly configure and deploy NextLabs' Compliant Enterprise®. In its specific configuration, Compliant Enterprise will unobtrusively collect data on user and information activities based upon the requirements you have provided.
4. After a period of data gathering, we will synthesize and provide you 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 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

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** to take advantage of our Information Risk Assessment Program for Endpoints.