Data Inventory Self-Assessment Guide

Data is one of the most valuable assets for any organization, where confidentiality, integrity, and availability (CIA) are paramount to the ongoing performance and business operation. This guide will help IT or Admin personnel in small to mid-size organizations to perform a self-assessment of their data inventory. Follow the steps below to gain visibility into where your data is stored and what it contains.

Data Inventory and Data Classification

First, we must identify and inventory the locations of data across the enterprise and pinpoint the sensitive data.

How do you create a Data Inventory?

Step 1: List all the locations where data is stored:

- ☐ **Servers:** Document the types of servers (e.g., database servers, file servers) and their locations.
- ☐ **Databases:** Identify different databases and their specific purposes (e.g., customer data, financial data).
- ☐ **Cloud Storage:** Note any cloud storage solutions in use (e.g., Google Drive, OneDrive, AWS S3).
- ☐ **Local Machines:** Include data stored on employee workstations or laptops.
- ☐ **Other Storage Locations:** Identify additional storage locations such as external hard drives, USB sticks, and backup tapes.

Step 2: For each storage location, gather details about the types of data stored:

- ☐ **Data Types:** Identify whether the data is structured (e.g., databases) or unstructured (e.g., documents, emails).
- ☐ **Data Volume:** Estimate the amount of data stored in each location.

Perform Sensitivity Classification

Next, we must classify the identified data sources bases on the sensitivity of the data and the protected information they contain.

How do you Classify Data?

Step 1: Identify data that contains sensitive information such as:

- ☐ **Personally Identifiable Information (PII):** Names, addresses, Social Security numbers, etc.
- ☐ **Protected Health Information (PHI):** Medical records, health insurance details, etc.
- ☐ **Financial Data:** Credit card numbers, bank account details, etc.
- ☐ **Trade Secrets:** Intellectual property or similar assets (drawings, diagrams, designs, etc.) critical to the competitive operation of your business.

Step 2: Use classification labels for your data:

- ☐ **Public:** Data that can be freely shared without risk.
- ☐ **Internal:** Data meant for internal use only.
- ☐ **Confidential:** Sensitive data that should only be accessible to authorized personnel.
- ☐ **Restricted:** Highly sensitive data with the strictest access controls.

Data Classification Example

The following table is a simple example of information that should be collected as an output of data inventory and data classification.

Example of data inventory and classification:

Location	Data Type	Data Volume	Classification	Sensitive (Y/N)
\\Server1\shareABC	Customer Database	500 GB	Confidential	Yes
\\FileServerA\C$	Employee Documents	200 GB	Internal	Yes
Google Drive\UserX	Project Files	100 GB	Internal	No
Workstation\Employee1	Various	12 GB per workstation	Confidential	Yes
External Drive “AAA”	Backups	1 TB	Restricted	Yes

By following these steps, your organization gains better visibility into where enterprise data is stored and what data contains sensitive information. This self-assessment can help you understand your data landscape and lay the foundation for improving your data security risk management.

Regular updates and reviews of your data inventory are recommended on a quarterly basis to maintaining an accurate and up-to-date view.

NEED HELP? Give us a call at (978) 444-2224 or email at info@blueinksecurity.com.