

Backup

An important consideration for any organization is protecting company data through backup. Without a current backup, even companies that employ a mirrored hard drive configuration may only realize limited recoverability.

To help protect against data loss, Aras recommends that companies running Aras Innovator software plan for and implement regular system and data backups. This plan includes the following:

- The purchase of a dedicated backup device and media.
- An appropriate backup schedule.
- Periodic test restores to verify backup integrity.
- Off-site storage of current or recent complete system backups.

A backup plan should also include an associated plan for restoring the data.

Importance of Backup

Regular backup of hard disks prevents data loss and damage caused by hard disk failures, power outages, virus infection, and many other possible computer problems. Backing up program files, databases, vault storage files, and configuration files on your servers is vital to planning a reliable and functional operation. You must back up your data so that you can restore important information or settings if problems occur.

Numerous unexpected events can cause data loss. Natural disasters, power outages, theft, user error, viruses, and hardware failures are all potential causes for partial or total data loss. Adequate backup and recovery procedures are your insurance against a serious disruption in business processes. The real cost of having a good backup plan in place can only be fully appreciated when critical data is lost.

The business impact of lost and potentially unrecoverable data is typically larger than the up-front investment of purchasing backup hardware and implementing a backup plan. Lost data and system downtime could result in lost revenue and the inability to conduct regular business. A valid and tested current complete backup can protect against data loss and substantially reduce recovery downtime.



Types of Backup

There are 3 commonly used types of backups:

- **Complete:** A complete backup copies all files in their entirety. With complete backups, you need only the most recent copy of the backup file to restore all the files.

Important

It is important to note that incremental backups must be restored in the order they were backed up.

- **Incremental:** An incremental backup copies only those files that were created or changed since the last complete or incremental backup. If you implement a combination of complete and incremental backups, you must have the most recent complete backup set, as well as all the incremental backup sets, to restore your data.
- **Differential:** A differential backup copies files that were created or changed since the last complete backup. If you implement a combination of complete and differential backups, you must have the last complete and differential backup sets to restore your data.

The following table compares the three most common types of backups.

Common Backup Types

Backup type	Advantages	Disadvantages
Complete	Easy-to-find files because complete backups are always on a current backup of your system. When restoring data, requires only the complete backup.	Most time-consuming when backing up. Backups become redundant, if files do not change frequently. Requires more disk, tape, or network drive space.
Incremental	Requires the least amount of data storage space. Least time-consuming when backing up. Backs up only those files that were added or changed since the last complete or incremental backup.	Difficult to find files because they can be on several different media. When restoring data, requires complete backup first and then each incremental backup in order.
Differential	When restoring, requires only the last complete backup and last differential backup. Less time-consuming than complete backups.	Longer restoration time than if files were on a single medium. If large amounts of data change daily, longer backup time is required.



Backs up all files that were added or changed since the last complete backup.

Storage Devices

Storage technology changes rapidly, so it is important to research the merits of various media before you decide. When selecting a storage device, consider drive and media costs, as well as reliability and capacity.

Media Types

The most common type of storage medium for backup is a removable media backup device (4mm DAT, Digital Storage Tape Drive, JAZ Drive, or similar high-capacity backup device). You can also store backups on another hard drive or network drive. However, off-site storage helps protect your data in the event of a disaster.

Size

An ideal storage device has sufficient capacity to back up the entire database and can also detect and correct errors during backup and restore operations. It is important to consider future demands when determining media size requirements.

Number of Media Units

Be sure to purchase enough media units to implement your backup plan for one year. For example, if you are using a tape backup method, you should consider how many tapes you need over the course of a year and then purchase as many tapes as possible up front. You should also replace worn tapes per the manufacturer's recommendation. Failing to purchase enough media to implement your backup plan can potentially limit its effectiveness.

Speed

Consider the bus and media speed. Depending on the amount of data you need to back up, you may require a faster device.

What Needs to be Backed Up

Identify all data assets that should be backed up. For your Aras Innovator implementation, these assets include, but are not limited to:



- Database files
- Vault storage files
- Program files
- Configuration files

Conduct a review of projects and materials that are stored on central servers and mainframes in your facility to ensure that you have identified all required components.

