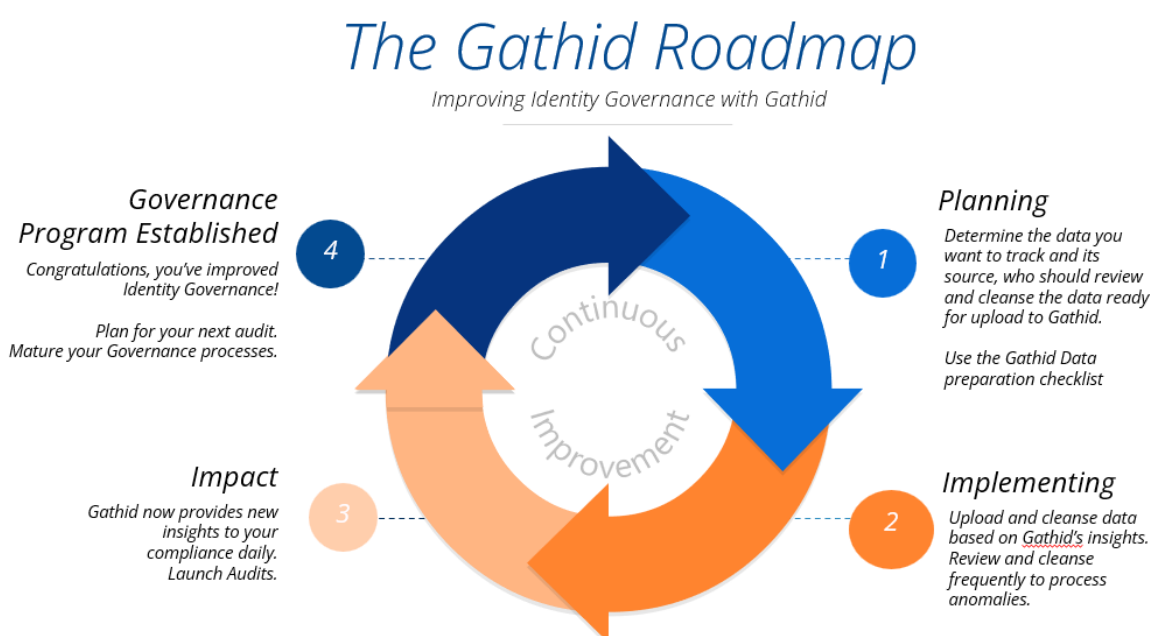


Gathid - Getting Started Guide

Welcome to Gathid – Let's get your Identity Governance Uplift underway!

Gathid is a powerful tool in your ability to control and monitor who has access to the environments and resources in your organization. Identity Governance is not only a technical matter, but also a business strategy, ensuring security, compliance, and efficient operations. But how and where to start? We've broken down the phases of an Identity Governance into three distinct areas, and depending on where you are with your own Customer Journey, you can start at the beginning, middle, or go straight to the benefits phase.



1. Planning

If you are new to Identity Governance, you will want to take a step back and consider the basics.

What data do you need to collect, track, and monitor? You might have a couple of data sources that you need to review, or you might have a more complex system with many data sources. At this point, you are jotting down the names of your data sources.

Where do I find the data I want to use? Once you've identified your data sources, determining the best way to extract data will be your next task. You can either send the data to Gathid by using one of the API connectors already in place, or you can upload a .csv file that contains your data. Whatever method you choose, if you can get your data into a spreadsheet, Gathid can read it and get the ball rolling.

Who should review the data? At this point, consider who would be the best set of reviewers, or

people who respond to the audit and keep an eye on the daily feed of data? The right answer is what will work best in your environment. It could be managers of people or areas, but you'll want someone informed enough to know who should and should not have access to your environments. And while you're identifying reviewers or responders, consider identifying secondary reviewers as well. These people will step in should your primary reviewer be out of the office or unavailable to review the data.

When should I review the data? Ideally, and as a best practice, you will have a process in place to review the data daily. Gathid presents new data to you every day, so having a group of reviewers to spot check this data will catch errors as they occur. Additionally, consider how often your organization can effectively support audits at a predetermined cadence. This can be monthly, quarterly, bi-annually, or annually.

2. Implementing

If you're ready to begin this phase, congratulations on completing the planning required for an effective set of processes to work with Gathid to ensure Identity Governance.

Ready to send your data? Before you do so, it is important from a quality assurance perspective, to double check your files. We've prepared a checklist to help you do so located here: [Data Preparation Checklist](#).

How do I send my data to Gathid? Gathid makes it extremely easy for you to send us the data you want to use in your Identity Governance processes. You will simply configure the data to automatically upload with Gathid's help through a data connector built specifically for your source system, or if one doesn't exist, by automated or manual system extract file transfer to the Upload Portal and upload them. To read more, [click here on how to determine the best upload method for you](#).

I can see my data in my Gathid UI, now what? Excellent progress so far. Now you will want to double-check to ensure that the format of the columns and how the data appears is exactly the way you want it to. If not, you will work with your Gathid representative to provide requirements for changes. Have a clear vision on what outcome you need based on your business process requirements and your Gathid representative will help you achieve this in the system.

What is data cleansing? Besides the format you want to see, it is also an important best practice to review the data and clean up anything that looks wrong or out of place. For example, some rows might be blank for an individual. This might be because an individual's name or email contains a typo, or there may be duplicate names or emails for the same individual. Gathid's modeling engine is going to find these and serve them up to you. Fixing these issues now, prior to a formal audit, enables a cleaner set of results for your reviewers to see.

3. Impact

Now that your data is visible and cleansing is in progress, audits can be initiated with confidence knowing that reviewers are only reviewing audit items that are clean and current.

How do I launch an audit? Gathid makes it easy for you to kick off an audit. Remember, you should also have a process in place for daily spot checks. But when ready to do so, you'll simply start your audit. It is helpful to send your reviewers a notice and let them know what to expect prior to launching your audit. You can find an example of a generic email message in this Knowledge Base library here: [How do I notify my audit reviewers to begin the audit](#). Once you hit the audit start button, your reviewers will receive notice that their Response pages are waiting for them. They will then indicate whether access for individuals is correct or not. There are also text boxes to record comments if access should be revoked (for example, someone may have just left the organization but the audit results show them to still have access). You can track the progress of your reviewers or responders so that you can see who has yet to complete their section.

How do I remediate audit findings? Your audit report will show you what needs to be corrected, and this is the exciting part. Congratulations on identifying items to be corrected, or remediated. You are well on your way to having an effective Identity Governance system in place. Once you have corrected all the findings from your current audit, you can review the entire process to plan for your next audit.

4. Enjoying the Rewards - Governance Program is Uplifted

Once you have concluded an audit and have a process in place for daily spot checks, you are able to attest that at this moment in time, your environments are clean! But this is just one snapshot at this particular moment. To sustain the momentum and continue to ensure that access is as it should be, you'll want to do the following:

How do I plan for my next audit? You've likely learned a great deal from the current audit. While the information is top of mind, begin planning for your next audit using the lessons learned during this particular one. You should already have a scheduled cadence for your audits, so depending on the frequency you've chosen, it is never too soon to set the stage for the next audit.

Any last suggestions? Your daily spot checks are your friend. Having an effective process in place along with a set of individuals responsible for achieving these spot checks, will ensure that your environments are accessed only by those individuals who are approved to do so.