ideiio

What is Identity Lifecycle Management?

2021 | Whitepaper | v1.0

ideiio.com

Introduction

Identity Lifecycle Management (ILM) is part of a wider set of capabilities known in the industry as Identity Governance and Administration, or IGA. Although sometimes the terms are used interchangeably, strictly speaking IGA solutions include ILM capabilities plus additional features such as identity certification, end user self-service and reporting.

In this whitepaper we will be focusing only on ILM, although ideiio is a full IGA suite with all of the mentioned additional capabilities.

In this 3-part series, I will help shed some light on what Identity Lifecycle Management is and how ideiio can help with your lifecycle management needs.

Part 1 – What is Identity Lifecycle

Identity Lifecycle Management is the practice of managing identity lifecycles. How's that for a circular definition? Identity Lifecycle Management can mean many things. It is really the practice of making sure people in your organization have the accounts and access that they need when they need it and making sure that access is removed when it is no longer needed.

There is a lot of jargon to sift through when looking at Identity Lifecycle Management. So let's start by taking a look at some of that jargon and putting some practical definitions on these obtuse terms.

Identity

An identity is simply a digital representation of a person in your organization. Identities can be employees, contractors, partners, customers, or anyone that you want to grant and manage access in your systems.

Lifecycle

An identity's lifecycle encompasses all of the things that happen to an identity that need to be tracked and managed. In general, this is typically broken down into 3 high level lifecycle events: joiners, movers, and leavers.

Joiners

Joiners are identities (people) that are joining your organization. These could be new employees that have just been hired, or customers that have registered on your website. This is the first touchpoint for an identity in your Identity Lifecyle Management process.

Movers

Movers are identities that are changing in some material way. Maybe an employee has changed departments and needs different access, they have changed their name through marriage or divorce, or a partner organization has increased their vendor offerings and needs additional access.

Leavers

Leavers are identities that are leaving your organization. This could be an employee who is retiring, a vendor that has been replaced or any other situation where you need to end the relationship between the identity and your organization.

Provisioning

Provisioning is the act of creating accounts or providing access for an identity in an IT system. When a joiner is added to an organization, we need to provision access for that user in the email system, for some file shares, in the CRM system, or whatever systems or applications they will need to fulfill their role in your organization.

Deprovisioning

Deprovisioning is the opposite of provisioning. It is the act of removing access, removing accounts, or disabling accounts for identities. When a mover changes their role in your organization, you will want to deprovision access that they needed for their old role and then provision access for their new role. When a leaver is ending their relationship with your organization, you want to deprovision all of their access. This allows you to maintain the security of your system and allows you to free up unused licenses.

Resource

A resource is simply something for which you want to manage access. A resource might be an application, a file share, or even physical access like access to the parking garage or company fitness room.

Role

A role is simply a logical collection of access that can be granted to identities. Roles can be based on job function, location, reporting structure, or whatever makes sense to your organization.

Entitlement

An entitlement is a specific privilege or access right within a resource. An example would be a time sheet application with permissions to enter time, approve time, and create job codes. The time sheet resource might have discretionary entitlements of time entry, approval, and administration.

Now that we are speaking the same language, in Part 2 we will take a look at some Identity Lifecycle Management use cases things to consider with an ILM project.

Part 2 – Use Cases

If you missed it, take a look at Part 1 of this series for an overview of what we mean by Identity Lifecycle Management and some definitions of common terms. Now that we understand the basic definitions let's take a look at some example use cases.

Identity Lifecycle Management can apply to any type of user that you have in your organization, employees, contractors, partners, customers, students, … For now, let's focus on the most common use type, employees:

Employee Onboarding (Joiner)

When a new employee is hired, they need to have all of their IT accounts created and be given access to all of the required systems. They will probably need an email account created, they need to have accounts created in any IT system they will use, they also need to be given access to appropriate file shares and other resources.

Obviously, not every new employee should be given the same access. In addition to provisioning a baseline set of access that all employees get, often referred to as birthright access, employees will need access specific to their job function.

How can a Lifecycle Management System help?

A new employee's journey usually starts with HR. The HR team ensures the new employee gets paid so everyone is motivated to make sure that process happens promptly and accurately!

A lifecycle management solution will monitor the HR system to look for new employees, then automatically provision access for the new employee. Employee access can be evaluated based on access control policies to ensure the new employee gets exactly the access that they need. If accounts are needed in external systems, those can also be provisioned in accordance with the access policies applied to the new user.

A good lifecycle management solution will ensure that a new employee has all necessary access to email and other systems set up from day one of their employment so can start productive work immediately – a zero-day start.

Employee Job Changes (Mover)

When an employee moves within the company, changes are often required to their access. A user switching departments or changing their job function will typically require new access to be granted to enable them in their new role. In order to restrict access to only those that need it and ensure overall system security any access that the employee no longer needs should be removed. This will ensure employees don't gather more and more access as they progress in their career (access creep), ending up with access and permissions that they don't need. Access creep over time is a huge security risk to the company.

Why is having too much access a problem?

When an employee has more access than they need to do their job their security risk increases. Risks from employees with granted access are referred to as insider threats. Insider threats can come in two forms: intentional and exploited. Intentional threats occur when a user with access in a system decides that they want to use that access to do something that they shouldn't. That could mean stealing data, misusing resources, sabotaging systems, or any number of other bad deeds.

Even if an employee is completely trustworthy and has no ill intent, having too much access presents security risks through exploited threats. For example if that employee gets hacked or their password gets compromised, then external bad actors can use that entry point to get into your systems. The more access available at the entry point, the easier it is for them to access your data and wreak havoc in your systems.

How can a Lifecycle Management System help?

A lifecycle management system can help ensure that a user has the access they need, and only what they need, by automatically provisioning and deprovisioning access based on defined access control policies. As with when a new employee is onboarded the job change is typically driven by the HR System. When the employee's record is updated with a new job or when a job is removed from their record the lifecycle management system will automatically see that change and make the appropriate changes to the employee's access. Old access that is no longer needed can be removed to ensure the user doesn't have more access than they need, and any new access that they need for their new job can be added.

Part 2 – continued

Employee Offboarding (Leaver)

All good things come to an end. Eventually, an employee will need to leave the company. When that happens it is important to remove any access that the employee has to ensure they can't get to data or systems that they shouldn't and to close any potential security risks. You will also want to ensure access is removed so you aren't paying for software licenses in SaaS systems for employees that no longer work for your company.

How can a Lifecycle Management System help?

As with most of our employee lifecycle, the HR system initiates the leaver process. The lifecycle management system will again be monitoring the HR system for any changes. When a user's employment is terminated their access needs to be removed. Automated workflows in the lifecycle management system can be used to do other required tasks as well, for example, notifying managers or opening help desk tickets to reclaim hardware.

Part 3 – ideiio Lifecycle

If you missed it, take a look at parts 1 and 2 for some definitions of lifecycle management terms and some examples of lifecycle management use cases. ideiio Lifecycle provides a full lifecycle management solution to automatically handle these use cases. Let's take a look at how.

Employee Onboarding (Joiner)

ideiio bridge is the provisioning engine within ideiio and can monitor your HR System for any new employees. After the employee data is entered into the HR System bridge creates the user record in ideiio based on that data.

HR System	ideiio bridge	ideiio core
Employee data entered		
	Read from HR and write to ideiio core	
		Determine access to employee data
	Provision access to external systems	
		Send email to new employee manager
		Send welcome email to new employee

Fig. 1. Joiner Workflow

Fig. 2. Mapping Overview

Attributes from the employee's record in the HR System are mapped to corresponding fields in ideiio core. If necessary, ideiio bridge can transform the incoming data with transformation pipes – for example, maybe your HR system uses the UK date format, and you want to manage dates in US format – ideiio bridge can change the date format on the fly.

Part 3 - continued

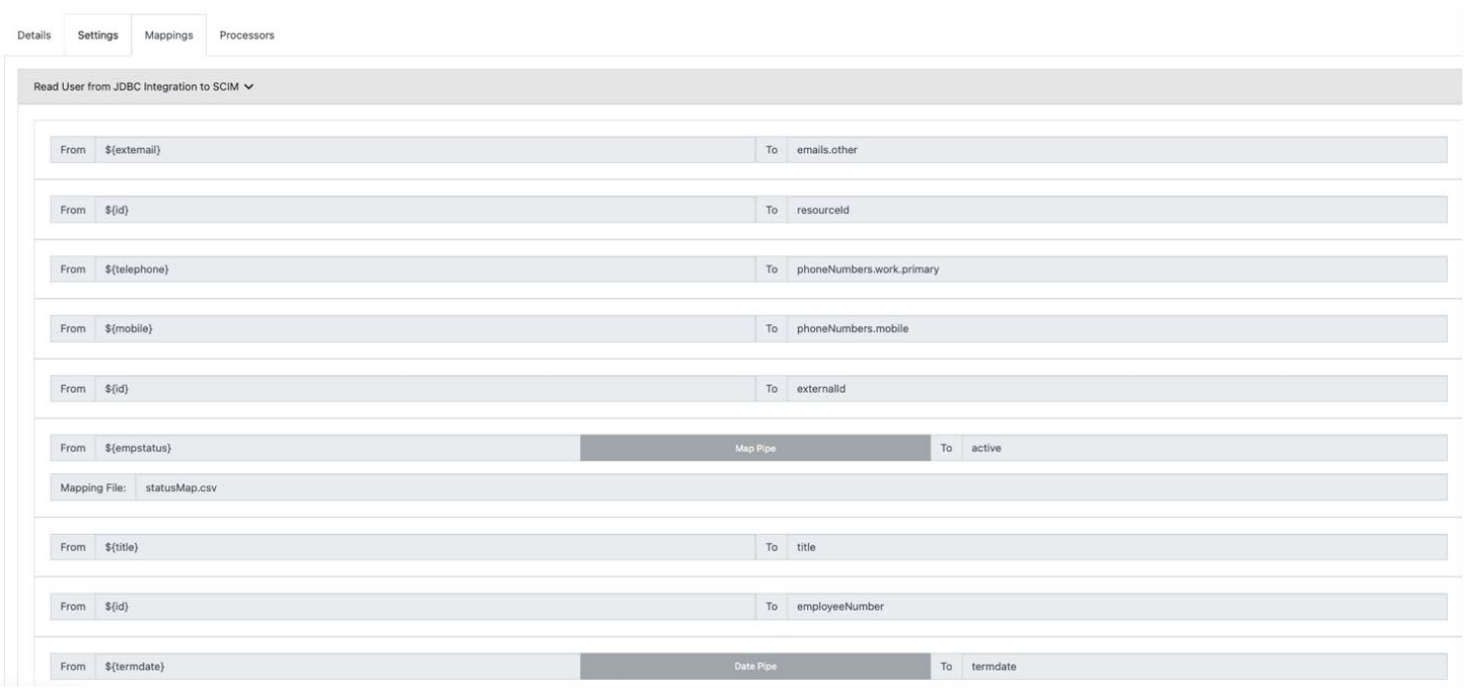

Fig. 3. Mapping Fields

Once the data is in ideiio core, the birthright access (a baseline set of access that all employees get) will be determined from the new employee's data and access roles will be assigned.

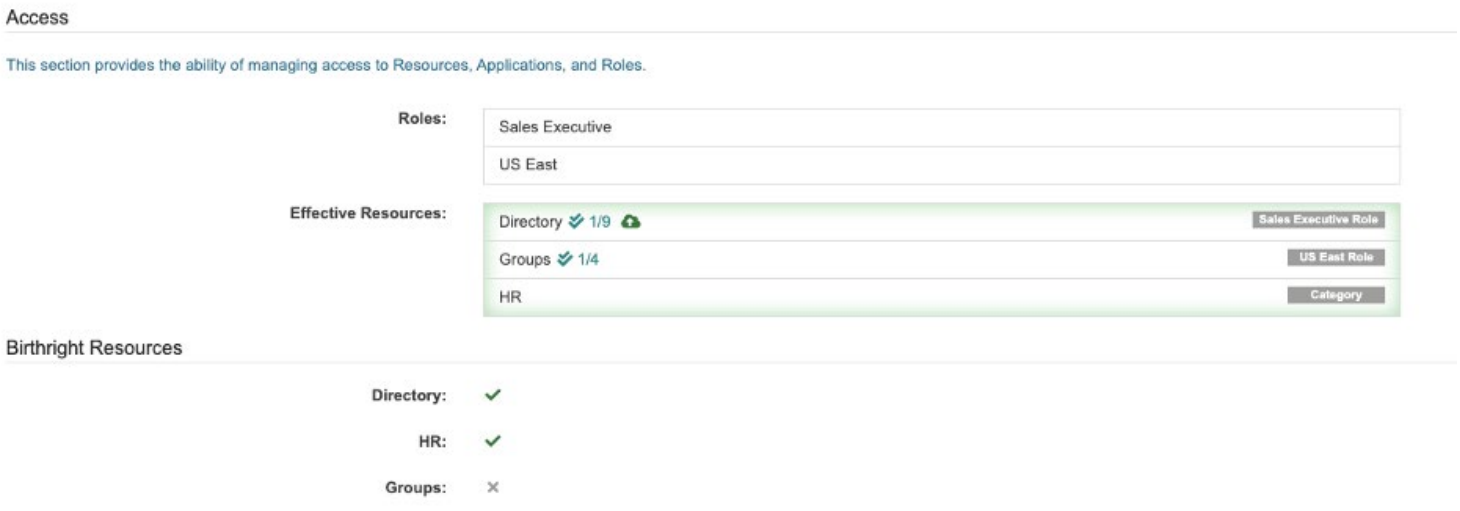

Fig. 4. Role & Resource Access Management

ideiio bridge will then create accounts in the external systems and provision access as needed for the birthright access and roles calculated by ideiio core.

Part 3 - continued

ideiio core workflows can be configured to send notifications to the employee's manager and to the new employee.

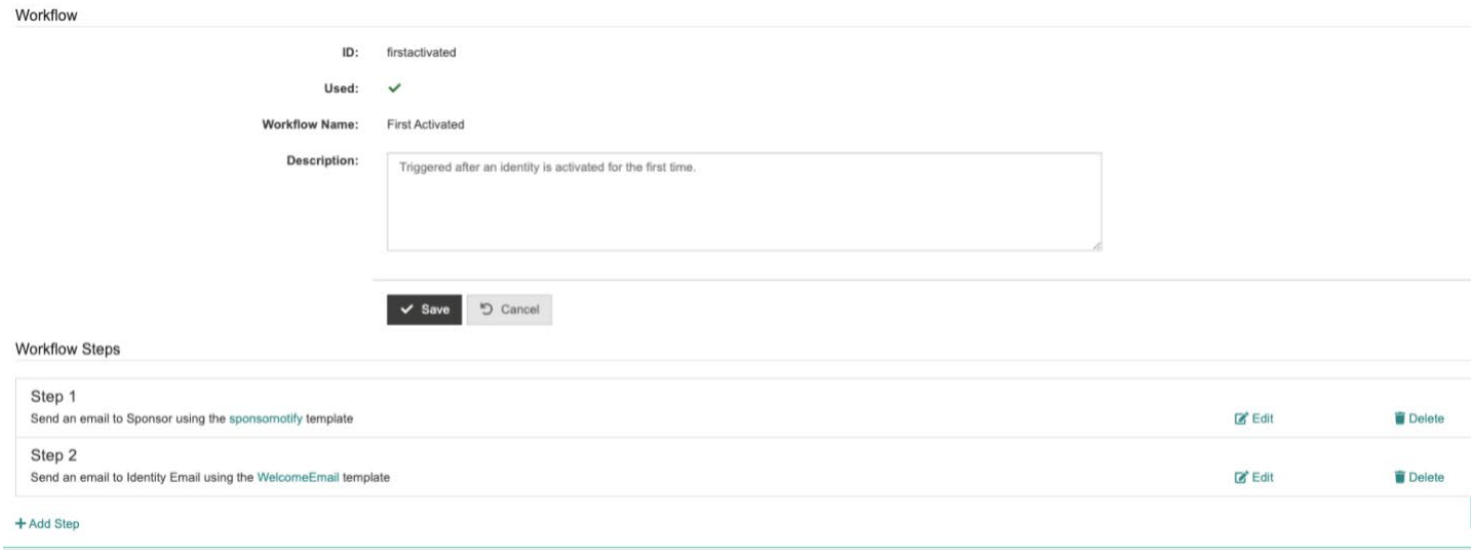

Fig. 5. Workflow Creation

Employee Job Changes (Mover)

With ideiio bridge continually monitoring the HR System any changes are picked up and synchronized to ideiio core. ideiio core will determine if any access changes are required when an update is detected. If updates to access are required, ideiio bridge will provision or deprovision access as needed.

HR System	ideiio bridge	ideiio core
New job entered in HR		
	Read from HR and write to ideiio core	
		Determine new access based on employee data
	Provision new access to external systems	
		Send notification to user of new access
Old job removed in HR		
	Read from HR and write to ideiio core	
		Determine access to be removed from user data
	Remove access that is no longer needed	
		Send notification to user of access changes

Fig. 6. Mover Workflow

Part 3 - continued

Workflows can be tied to any lifecycle event for a user and provide custom processing based on changes in employee data. Over 45 out of the box workflows provide default behavior for these lifecycle events. All of these workflows can be customized.

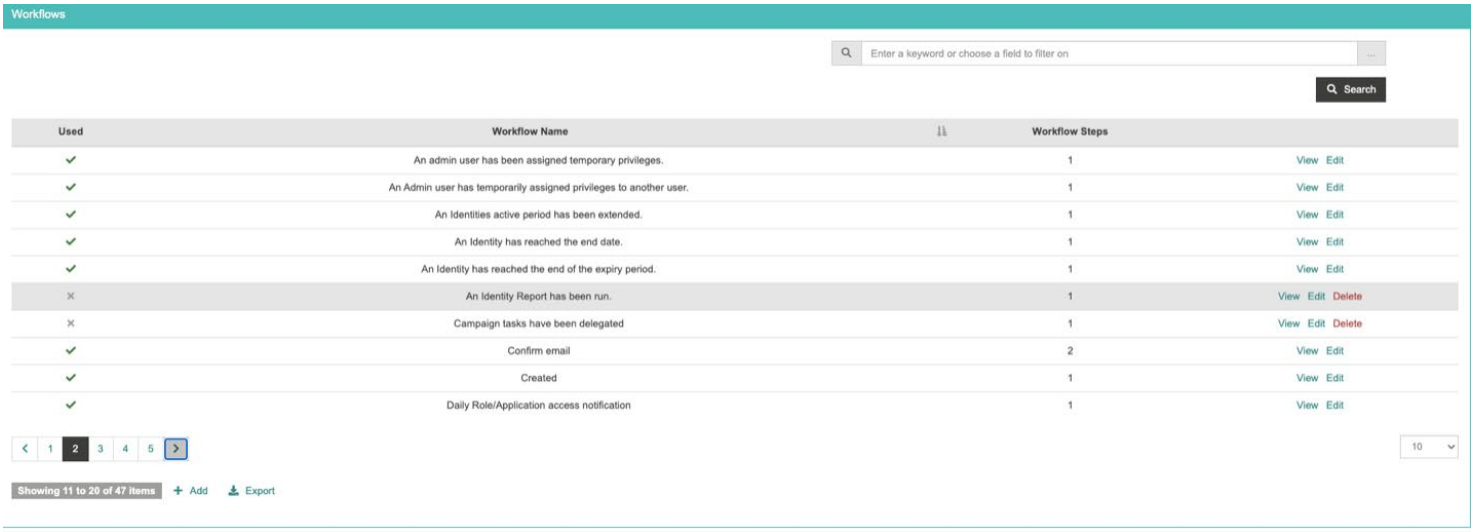

Fig. 7. Out of the Box Workflows

New workflows can also be added based on lifecycle or system events.

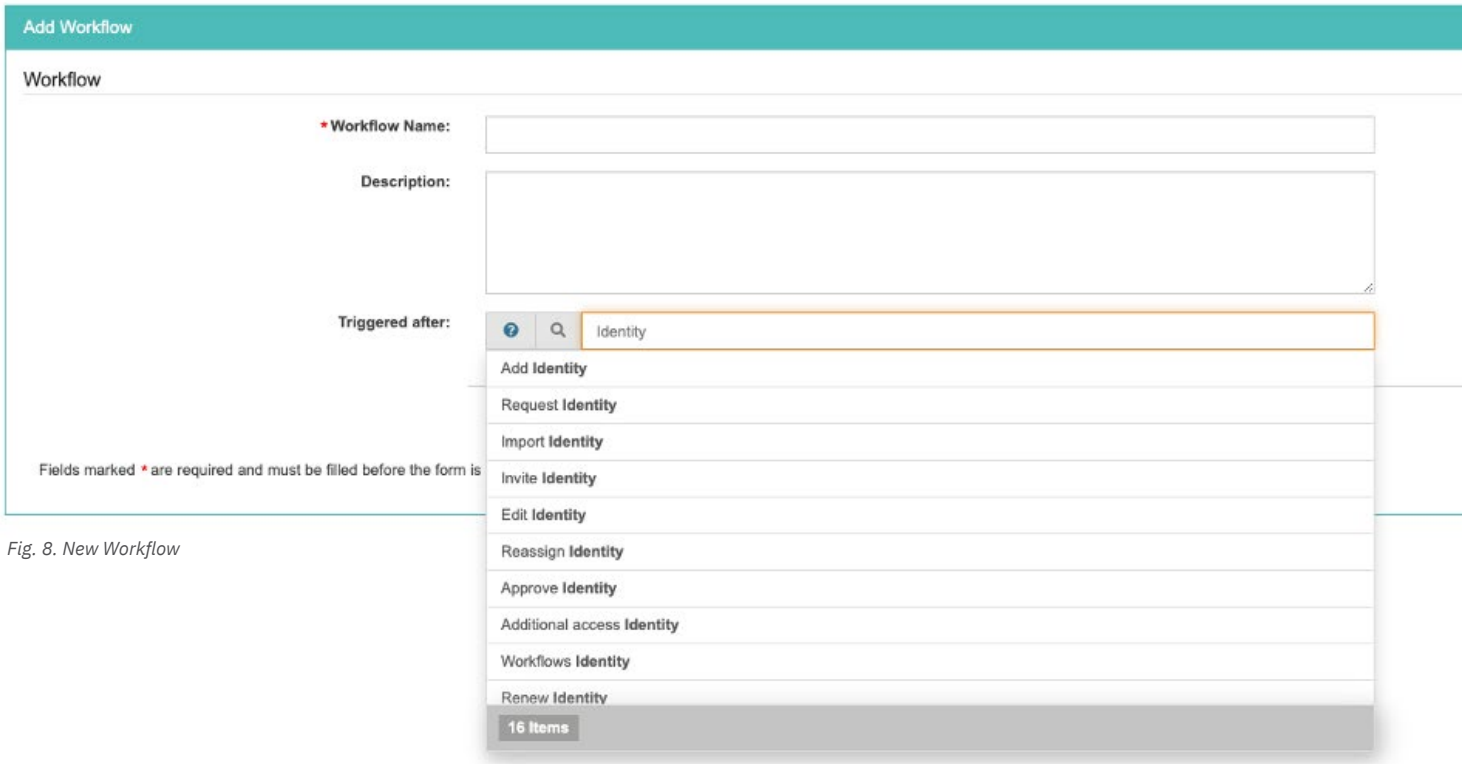

Fig. 8. New Workflow

Employee Offboarding (Leaver)

When an employee is terminated in the HR System ideiio bridge will see the change in the employee's status and synchronize the data with ideiio core. ideiio core will calculate access changes (typically removing all access) and ensure that the changes are provisioned or deprovisioned through ideiio bridge.

As with all transactions, ideiio core will ensure any changes to access are fully audited in case you need to review when a terminated user was identified and when and what provisioning events occurred.

HR System	ideiio bridge	ideiio core
Employee terminated		
	Read from HR and write to ideiio core	
		Access removed from user
	Access deprovisioned in external system	
		Send email to employee manager

Fig. 9. Leaver Workflow

Date	Entity	User	Audited Action	Object	Result	
03/03/2021 23:59:11	Identity	Local Administrator	View Identity	Donald Moore	✓	View
02/25/2021 19:33:06	Identity	Local Administrator	Provision Identity	Donald Moore	✓	View
02/25/2021 19:32:27	Identity	Local Administrator	View Identity	Donald Moore	✓	View
02/25/2021 19:32:26	Identity	Local Administrator	Terminate Identity	Donald Moore	✓	View
02/25/2021 19:30:09	Identity	Local Administrator	Provision Identity	Donald Moore	✓	View

Fig. 10. Audit View

Conclusion

I hope this series helps provide some understanding of Identity Lifecycle Management. These capabilities and use cases are the heart of a full Identity Governance and Administration (IGA) solution such as ideiio.

To find out more information about ideiio, visit us at ideiio.com or follow us on twitter at twitter.com/ideiio

Author

Matt Berdine is the Chief Product Officer of ideiio, a world leading Identity Governance and Administration software company. ideiio is Headquartered in Manchester, UK and Matt heads up the Development team in Colorado Springs, USA. He is regarded as a leading authority on Identity Lifecycle Management (ILM) and Identity Governance and Administration (IGA).

About ideiio

We are industry experts who have come together with the bright idea of making Identity Lifecycle Management simpler for our customers.

For more information:
hello@ideiio.com
ideiio.com

EMEA & APAC

8 Exchange Quay
Manchester
M5 3EJ, UK

t. +44 (0)161 204 7788

North & Latin America

1755 Teslar Drive
Suite 206, Colorado Springs
CO 80920, USA

t. +1 719 453 1067