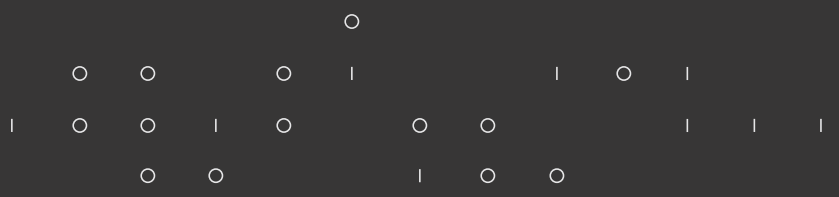
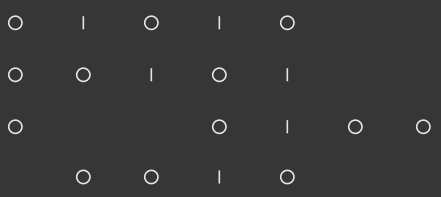


ideiio



Identity Governance and Administration.

Making sense of multiple identity lifecycles in academia.

2019 | Whitepaper | v1.0

ideiio.com

Contents

Introduction

The modern enterprise interacts with many kinds of individuals, each with a distinct digital identity, and each with a different digital journey. At the minimum, most companies must manage digital identities for their staff and customers, but other categories can include external users such as affiliates, B2B customers or supply chain (users from other organizations) or, in the case of universities – students.

Each of these types of individual has a pattern which describes their association with the organization over time – how they make first contact, form a formal relationship with the organization, maybe change roles and eventually end their association. Thinking about two examples – staff and customers – we can easily see that the journeys are different. Staff usually start their journey with a job offer and a record in the HR system; customers usually start their journey with a purchase and filling in a registration form.

The differences in the needs of each type of digital identity don't stop there however. Each category of identity has different requirements for security, access control and governance. For example, with staff who will have access to controlled and sensitive information we will typically have much more stringent security and governance controls; for students, we want to emphasize productivity and for the experience to be easy and frictionless.

Managing the identity lifecycles for all these types of individual at once can be challenging. In this whitepaper we will explore the different requirements of the identity lifecycle for each type of constituent, and which key features are needed in an Identity Governance and Administration system to manage the lifecycles effectively. Finally, we will explore how ideiio provides a quick to value way of managing multiple identity lifecycles in a single identity management platform.

Glossary of terms

Identity Governance and Administration (IGA)

The generic name for technology which helps organizations manage digital identities that interact with the enterprise, and their access permissions. IGA technology helps organizations answer the questions 'who should have access to which resources, when they should have that access, and who decides?', as well as automating the process of creating and maintaining digital identities. ideiio is an Identity Governance and Administration platform.

Identity lifecycle

The journey of a digital identity through its association with an organization, describing how the identity is created, how its access is modeled and managed, and how it is decommissioned when the association comes to an end. The identity lifecycle differs for different kinds of individuals i.e. the identity lifecycle for a member of staff may be different than for an affiliate.

The identity lifecycle – create, update, delete

The term 'identity lifecycle' refers to the process an organization must go through to manage a digital identity for an individual, from the start of their association with an organization through to the end – 'cradle to grave'. Essentially, the process can be boiled down to the commonly used acronym 'CRUD', which stands for 'create, update, delete'.

Taking each of these in turn, we can see how these stages map to the journey of a digital identity.

Create

This is the first action that must take place when an individual starts a digital relationship with the organization – a digital identity must be created recording key identity information (or 'attributes') about that individual. This can happen in several ways, ranging from manual entry by an IT administrator, through automated synchronization from an 'authoritative source' such as a HR system to self registration via an online form. Different methods are appropriate for different types of identity. For staff, it is important that the identity data we hold is accurate and complete to enable the organization to comply with its duties as an employer. For customers or external users, the completeness or accuracy of the data is less important. Of course, we always desire accurate data, but for these kinds of users the effort involved in ensuring accuracy may be outweighed by the benefit of quickly and easily creating an identity record (e.g. through self registration).

Update

Updating of the identity record is something that takes place throughout the individual's association with the organization – however the pattern and frequency of the updates will vary significantly across different types of identity. Students, for example, will tend to have a 'lighter touch' digital relationship with the university, with minimal changes to access once course selection has been set. With students acting more as a 'consumer', changes to access are less likely to have security implications or require approval. For staff, the relationship is much deeper and constant. Over time the member of staff is likely to change role or take on additional responsibilities which are likely to require changes in their access to systems – and these changes are likely to require approval from a manager, and to be checked over time. In this model, updating is a core part of the identity lifecycle and a vital part of the organization's security posture as well as productivity driver.

Delete

When the relationship with the organization comes to an end, maybe due to a termination of employment or the end of a contract, the digital identity must be decommissioned somehow. Again, this can take multiple forms depending on the type of identity. For students at a university for example, it is common for the decommissioning of a digital identity to be a drawn-out process, taking place in stages over months. Starting with disablement when a student's course ends, there is then often a period of months while data is archived before the identity is finally deleted; in many cases, the digital identity may even be retained with reduced access as an 'alumni' account. For staff, this decommissioning is often tied to a date, but can in some cases be instant (in the case of abrupt termination). For customers, depending on local data protection legislation, there may be no delete 'event', unless the customer themselves requests it.

The staff lifecycle

The nature of the relationship between members of staff and the organization drives the requirements of the staff lifecycle.

It is essential that the organization has up to date information about the individual for legal, contractual and operational reasons. Therefore, the identity lifecycle is driven automatically by an 'authoritative source' which the organization has deemed to hold the most accurate data. Typically, this authoritative source is the HR system, and the HR team are ultimately responsible for maintaining this data. Any data entered into the HR system, and any modifications thereafter, will be synchronized into the identity management system to drive the identity lifecycle.

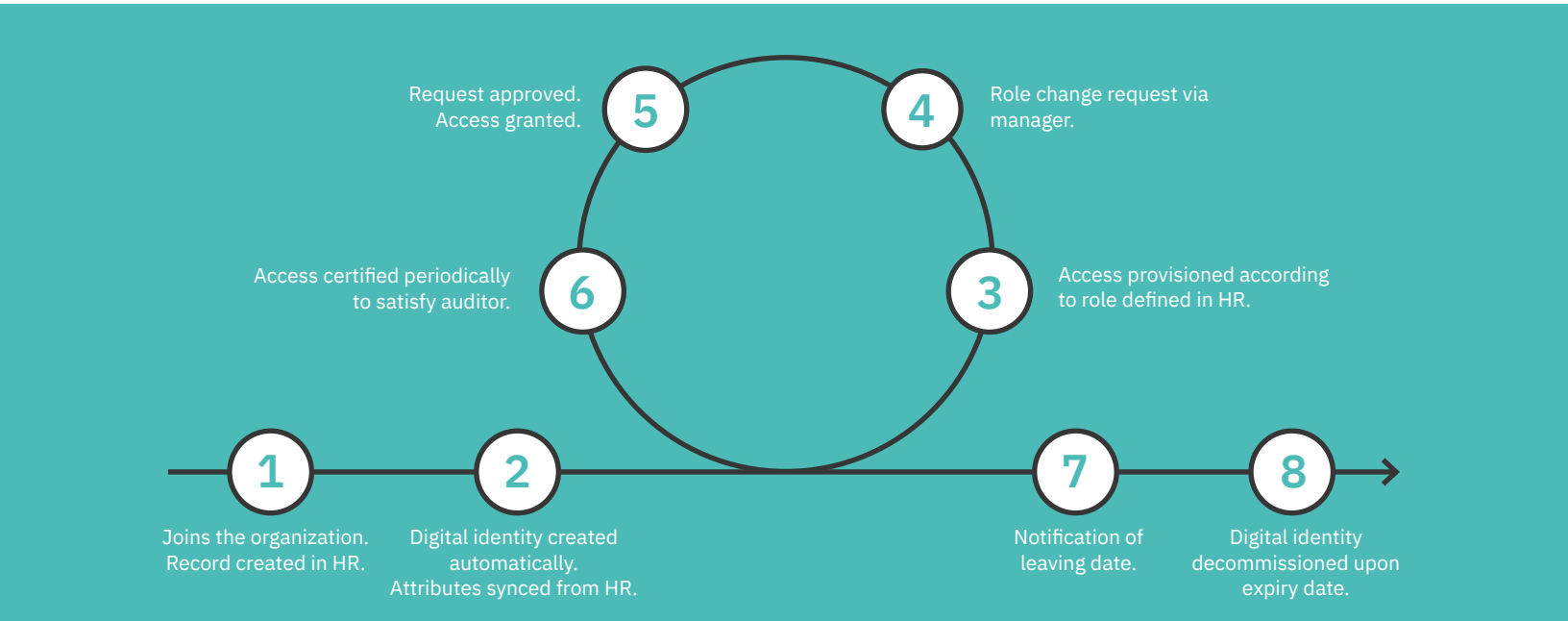
Typically, members of staff have highly focused responsibilities which requires access to a subset of applications. Some of these applications will be common across all members of staff, such as an email address ('birth right access'). Other applications will be specific to their responsibilities, or role(s). A core part of the identity lifecycle for staff is ensuring that their access to applications and systems remains appropriate to their roles always. Crucially, this means removal of access when a system is no longer required, maybe due to a change in role.

Whether due to operating in a regulated industry, or simply down to good corporate practice, it is important that access to data is tightly controlled to protect company intellectual property. Therefore, typically the staff lifecycle will involve a system of workflows whereby application owners can approve or decline access to their application, ensuring that access is limited to those that really need it.

Further to the point above, it is important to check regularly that access is still required; for example, if an individual has changed to a new role and no longer needs access to an application but the relevant administrator has not been informed, there is a risk of protected data being exposed to an individual who does not need it. Therefore, the staff lifecycle typically involves a process of 'certification' whereby on a regular basis, managers are requested to confirm that the individual still needs the access they have been granted; if they do not, then the access can be automatically revoked.

Decommissioning of staff identities tends to be date driven, typically linked to the last day of employment. To protect corporate data, access must be immediately removed when the identity is decommissioned. In some instances, it is essential to revoke access immediately - for example, if a member of staff is abruptly terminated for misconduct. In this instance it is doubly important that all access is immediately revoked. Therefore, the staff lifecycle typically requires date based decommissioning, alongside immediate termination capabilities.

Fig. 1. The staff lifecycle



The student and alumni lifecycle

The student lifecycle shares some characteristics with the staff lifecycle, in as much as it is typically driven from an authoritative source – the Student Records System. However, thereafter the lifecycle is quite different, with an emphasis on productivity and a seamless experience to support the student's learning journey.

As for the staff lifecycle, it is essential that the university retains accurate information about the student for legal, operational and contractual reasons. It is also essential that students' access to university resources are linked to their enrolment status. Therefore, the student lifecycle typically starts when a record is created for a new student in the student records system. Any data entered into the student records system, whether relating to identity attributes or status, must be synchronized into the identity management system to drive the identity lifecycle.

One difference with the staff lifecycle is that the access to data and applications that a student needs is very much driven by their course enrolments as opposed to functional roles. A student enrolled on a maths degree, for example, requires very different access than a student reading English – whilst they may both have the same coarse-grained entitlements (i.e. access to the Virtual Learning Environment or VLE), their fine-grained entitlements will be driven by enrolments (i.e. access to the relevant modules in the VLE). Therefore, enrolments information is typically another core driver of the identity lifecycle for students; if course enrolments change then so must access, driven by the authoritative course enrolments data.

Given the nature of the student's role, the data they can access tends to be less critical than for staff; therefore, the emphasis on governance around granting access is lower than for staff – instead the focus is on a seamless experience and self service to enhance productivity. Unlike the staff lifecycle, this means there is little need for approval workflows for access requests, or for certification activities. Instead, access to applications will typically be provided in advance as 'birth right' or provided via self service on demand.

When the student finishes their course, the process of decommissioning is in many cases staged over time. Limited access and data may be retained for a period to enable the student to have access to their work. Additionally, it is common for student accounts to be converted to alumni accounts to enable a lifelong relationship between the student and the university. This change is more than a change of role – it is a fundamental change of category of digital identity, more akin to the relationship between a retailer and its customers – essentially a new identity lifecycle is initiated at this point – the alumni lifecycle.

The alumni lifecycle may be initiated automatically as described above; additionally, it may be appropriate to allow alumni to self register or be invited – maybe for historical alumni. The relationship with alumni will tend to be fairly static and focused on delivery of information and services from the university. Therefore, identity updates will typically be via self service, whether to add new online services or to update identity profile information (e.g. a new email address). The decommission phase of the alumni lifecycle will tend to only occur if the alumnus themselves requests that the relationship is terminated – otherwise the digital identity will persist.

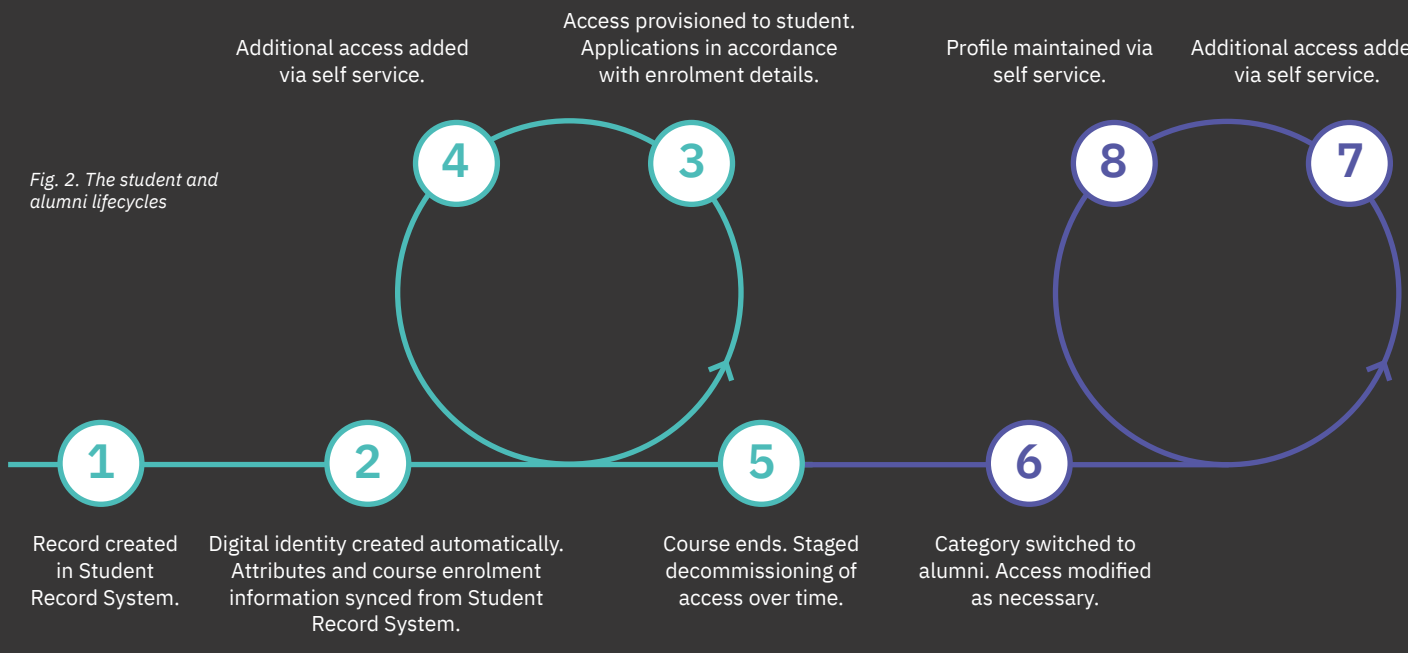


Fig. 2. The student and alumni lifecycles

The affiliate lifecycle

Modern universities interact with many different types of external users, ranging from contractors to conference delegates or walk-in library users. For most universities, at any one time there may be thousands of such external users, sometimes known as 'affiliates' – each type of affiliate may have different access and governance requirements which can make management of this particular lifecycle quite complex.

The affiliates lifecycle shares some characteristics with the staff lifecycle, as depending on the type of affiliate, the security and governance requirements can be even more important, as they do not have a permanent relationship with the organization. Additionally, given the many different types of affiliate which a university may need to interact with, a flexible role based access control (RBAC) model is essential to be able to model the different access and governance requirements which are appropriate to each type of affiliate.

However, the start and end of the affiliate lifecycle tends to be much 'fuzzier'. For example, HR may never know about the recruitment of an affiliate – often this activity takes place within the department where the affiliate will be working or providing a service. Therefore, the lifecycle is typically initiated outside of HR, by the recruiting manager. This may take place via an online form, or invitation and may include approvals workflows; crucially however, the creation of the identity is not driven by an authoritative source. Variations on this theme apply to all types of affiliates. For example for conference delegates, the lifecycle is likely to initiated by email invitation; for walk-in library users, an online form may be more appropriate.

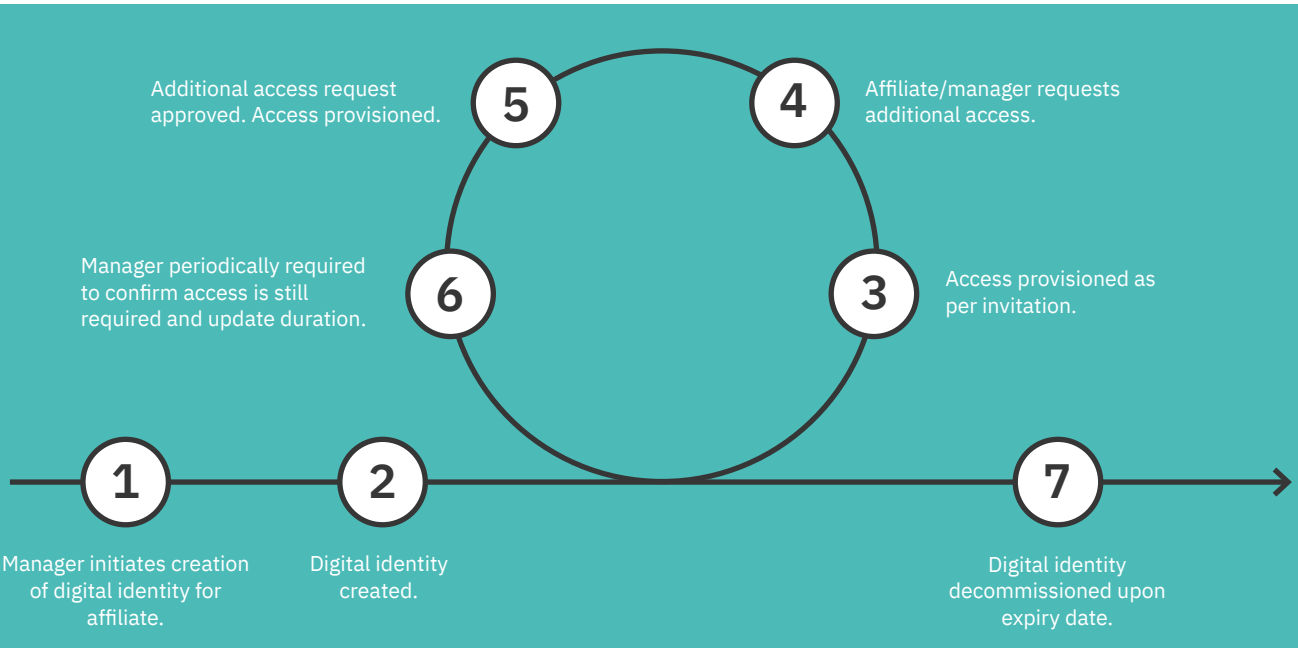
During the 'update' phase of the affiliates lifecycle, the process is the same as for staff. Access to applications and systems are automatically provisioned, either driven by information provided during the creation process, or by a request and approval workflow.

As for staff, certification of the identity is frequently required, except for identities for members of the public such as walk-in library users that do not have access to sensitive information. However, for affiliates, certification may well take place more frequently than for staff e.g. monthly. This is because often the organization may not hold a contractual end date for affiliates (as they may do for staff) and the end date may be indeterminate in any case e.g. in the case of an affiliate, it may be linked to an ongoing project which is experiencing delays.

Once an end date is established for an affiliate, the decommissioning process can proceed as for staff.

As affiliate data is unlikely to be driven by an authoritative source such as HR, providing a mechanism for affiliates to keep their identity attributes up to date may be very important. Therefore, profile management is a core part of the affiliate lifecycle.

Fig. 3. The affiliate lifecycle



Comparison of lifecycles

The section above described some of the common identity lifecycles prevalent within modern enterprises, highlighting some of the key differences with each.

The table below summarizes the key characteristics of various flows, showing the core features of an Identity Governance and Administration platform that are required to manage each lifecycle (Fig. 4).

Fig. 4. Comparison of different identity lifecycles

	Staff	Student	Affiliate	Alumni
Driven by external authoritative sources	X	X		
Delegated administration			X	X
Invitation			X	X
Self registration				
New account approvals			X	
Identity certification	X		X	
Identity roles	X		X	
Time based events	X	X	X	
Access requests	X	X	X	
Self service	X	X	X	X
Profile management	X	X	X	X

Features checklist for an Identity Governance and Administration platform

A description is provided below for each of these core features that should be present in an Identity Governance and Administration platform in order to manage the various identity lifecycles within a university.

Driven by external authoritative sources

This means that the Identity Governance and Administration platform can read identity events from an authoritative source of identity data, such as the HR system, and synchronize any changes resulting from these events in to the platform, and thereafter out to any connected applications. Typical events include identity creation, update (whether of identity data or role information)
and deletes.

Ideally, the Identity Governance and Administration platform should be able to synchronize identity data from multiple authoritative sources, recognizing that many organizations may have multiple such sources – for example, universities typically have a Student Record System for mastering student identities.

Delegated administration

Delegated administration is the ability for the administration of identities and their data to be 'delegated' away from a central function such as IT or HR to individuals or departments across the organization, or even to external organizations. This is typically useful for lifecycles which do not start with data mastered in an authoritative source (e.g. the affiliate lifecycle), where there is a need for the process of managing identities to be decentralized to remove bottlenecks and improve efficiency. Furthermore, by moving the administration of identities closer to the departments that will be working with these individuals, security and governance can be improved as the delegated administrators will have a broader appreciation and knowledge of the individuals working context and functional role.

Identity certification

Identity certification is a way of guarding against a build-up of 'zombie' accounts – or digital identities which belong to individuals that have left the organization but are still active. Such identities present a significant security and compliance risk to the organization, as the digital identity may confer access to critical systems and data, which could leak outside of the organization.

Identity certification typically works by requiring managers to 'certify' that individuals that they are responsible for still require their access, and that their access is still appropriate their role.

Different lifecycles may require different certification schedules – for example, it may be desirable to certify staff more frequently than students (in fact, students may require no certification at all). The Identity Governance and Administration platform should have the flexibility to define different certification policies for different kinds of users.

Identity categories

With reference to the affiliates lifecycle, there is often a need to apply different governance and access policies to different categories of identity within the same overall lifecycle; identity categories provide a way to achieve this.

For example, within the affiliates lifecycle, affiliates and conference delegates have quite different governance profiles; the duration of an identity is well defined for a conference delegate whereas for an affiliate it may be indeterminate. A conference delegate is unlikely to have access to any sensitive material so password complexity and identity certification regimes can be less stringent than for an affiliate, who may have access to corporate systems and data.

The ability to apply these different policies to large groupings of identities is crucial in a university setting where many different types of user interact with the organization, each with quite different profiles.

Invitation and self registration

For lifecycles where identities are not synchronized from an authoritative source, it is necessary to collect identity data some other way. Self registration flows are extremely useful in this regard, whether by an online form or via a link to a form sent via email invitation.

The benefit of these approaches is that administration is minimized, and collection of identity data is delegated to the individual themselves. Forms and/or invites can be processed in advance of a start date or on demand when access is needed.

A further advantage is that passwords can be set as part of the registration flow, rather than being generated by the system; this removes the need to implement a workflow to communicate an initial password to a new user.

Identity roles

Identity roles provide a way for an organization to map functional roles (i.e. what job or jobs an individual does for the organization) to the digital resources that they need to perform those functional roles. For example, a lecturer may need admin access to the Virtual Learning Environment and library systems, whereas a finance administrator would need access to the finance applications. Roles provide a means to manage these assignments efficiently, without needing to manage many 'one-to-one' assignments between individuals and applications. Additionally, when an individual changes job, their identity roles can be automatically updated by the Identity Governance and Administration platform, and their access will be updated accordingly.

Identity roles capabilities are particularly vital for staff and affiliate lifecycles; they may be useful for the student lifecycle as well depending on local business rules – however typically student access is more homogeneous than staff access.

Approval workflows

For some lifecycles, it may be desirable to carry out an approvals workflow before commissioning a digital identity and granting access to systems. This is not typically a requirement for lifecycles driven by an authoritative source, as it is usually determined that the act of adding an identity record to the authoritative source by an authorized user is a form of approval.

Where an authoritative source does not form part of the lifecycle, it is a good idea for a manager to review requests for new digital identities, and to approve or reject them prior to access being granted to core systems. This should be implemented via a workflow system to ensure that transactions are tracked, not missed and acted upon in a timely manner.

Time based events

For the staff and student lifecycles, the ability to process identity events on a time basis is essential.

For staff, frequently major identity events such as decommissioning of an identity are tied to future dates such as the end of a contract or a known leaving date. For students, there is often a staged decommissioning process based around the amount of time from the end of a study program (i.e. reduce access on day 1, disable after 90 days and delete after 180 days).

The Identity Governance and Administration system should be able to process such events automatically when the appropriate time comes.

Access requests

Access requests are an important part of the staff and affiliate lifecycles and may be relevant to the student lifecycle as well depending on how the university is organized. Access requests provide flexibility, by allowing either the individual or a manager to request additional access beyond birth right access, or access inherited from identity roles.

This is important, as it is not always possible to accurately or efficiently model all the roles within an organization – there are always exceptions, for example if a member of staff is temporarily seconded to a project outside of their normal role.

Providing the capability for ad-hoc requests, alongside the ability for application owners to review and approve requests provides a fundamental part of successfully automating identity lifecycles.

Self service

Self service is like access requests, with the difference being that self service allows users to simply add access, without needing to go through a request process. This is very useful for lifecycles which model a 'looser' relationship with the organization and where access governance is less important (e.g. the alumni and student lifecycles) but could be important across all lifecycles by granting easy access to non-critical applications. Allowing users to help themselves is a key part of delivering a seamless digital experience to users.

Profile management

Profile management refers to the ability to allow end users to manage their own identity attributes – for example, to update their email address or home address.

This is most important for lifecycles which are not driven by an authoritative source (e.g. affiliate and alumni lifecycles) as they allow the end user to become authoritative for their own data.

However, it is also a core feature for lifecycles driven by authoritative sources, as it provides a way for keeping identity data up to date which may not be otherwise updated in the authoritative source – a typical example would be personal email addresses.

Conclusion

Built on 25 of years of experience working with the complexities of the academic sector, ideiio is an Identity Governance and Administration platform, providing both automation of the joiners/movers/leavers process alongside built in identity governance workflows. Thus ensuring organizations can enable their users have the right access to applications and data.

ideiio provides built-in functionality to support all the identity lifecycles described in this whitepaper with the additional benefit of being an out of the box solution. In addition, it enables organizations to flexibly manage the identity lifecycle for all their constituent users in a single identity management platform.

Not only is ideiio stacked with features there are also multiple benefits for deploying the solution:

Reduce business risk
Satisfy internal audit requirements with compliance and governance workflow.

Achieve regulatory compliance
Eliminate manual efforts on IT audits and provide a more secure environment.

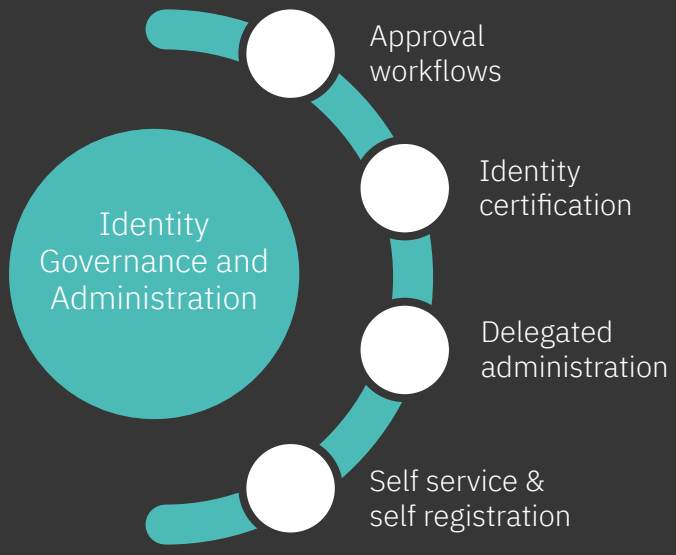
Reduce operational costs
Reduce IT support costs by empowering users with self service workflows for account registration, profile management and password/username recovery.

Enhanced user experience
Frictionless secure onboarding and offboarding for an enhanced user experience.

Rapid deployment
Deploy in weeks rather than months.

Quick to value
Cost effective license model.

How it works



Find out more here.

Download the data sheet here.

Getting started
Sign up for your free tenancy and experience the ideiio online demo here.

ideiio
intuitive identity

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