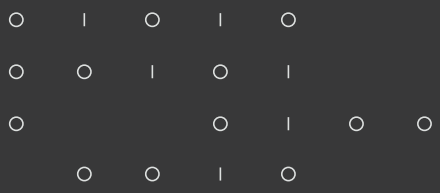
ideiio



Making Sense of Identity Lifecycles.

2020 | Whitepaper | v1.0

ideiio.com

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 contractors, B2B customers or supply chain users from other organisations.

Each of these types of individual has a pattern which describes their association with the organisation over time – how they make first contact, enter into a formal relationship with the organisation, 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. 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 customers – we want to emphasise ease of use and for the experience to be frictionless to encourage engagement.

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 how ideiio provides a quick to value way of managing these lifecycles in one IGA system.

The identity lifecycle – create, update, delete

The term 'identity lifecycle' refers to the process an organisation must go through to manage a digital identity for an individual, from the start of their association with an organisation through to the end – sometimes known as 'from 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 organisation – 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 synchronisation 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 organisation 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 takes place throughout the individual's association with the organisation, however the pattern and frequency of the updates will vary significantly across different types of identity. Customers, for example, will tend to have a 'lighter touch' digital relationship with the business, with minimal changes following initial registration; as customers are consumers of services, 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; 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 organisation's security posture as well as a productivity driver.

Delete

When the relationship with the organisation 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 in an enterprise, however, 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 organisation drives the requirements of the staff lifecycle.

It is essential that the organisation 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 organisation 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 synchronised into the identity management system to drive the identity lifecycle.

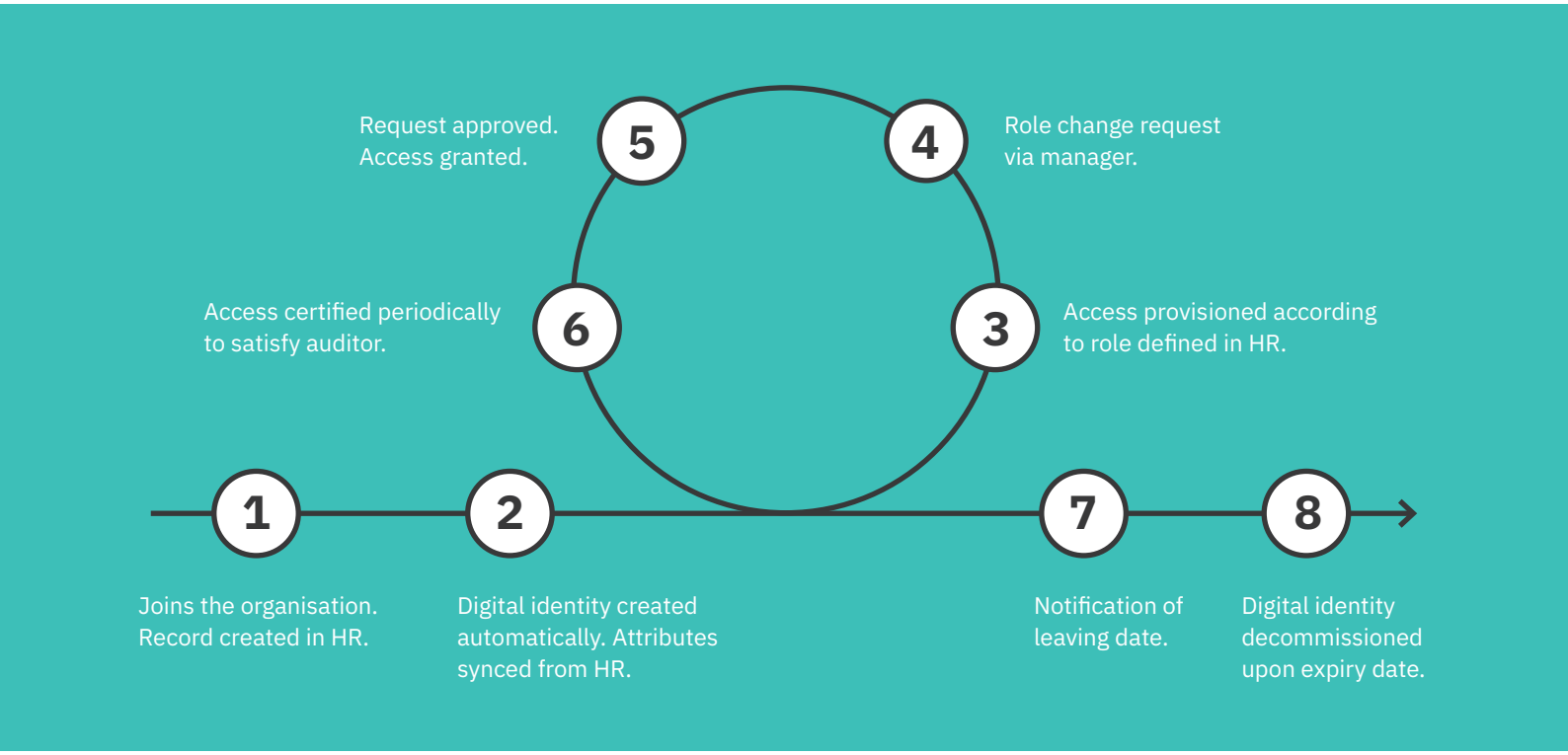
Normally, members of staff have highly focused responsibilities which requires access to a subset of applications. Some of these applications will be common across all members of staff, such as an email address ('birth right access'). Other applications will be specific to their responsibilities, or role(s). A core part of the identity lifecycle for staff is ensuring that, at all times, their access to applications and systems remains appropriate to their roles. 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 a particular 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 contractor lifecycle

The contractor lifecycle shares some characteristics with the staff lifecycle, as the security and governance requirements are arguably even more important with a contractor who does not have a permanent relationship with the organisation.

However, the start and end of the contractor lifecycle tends to be much 'fuzzier'. HR may never know about the recruitment of a contractor – often this activity takes place within the department where the contractor will be working or providing a service. Therefore, the contractor 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.

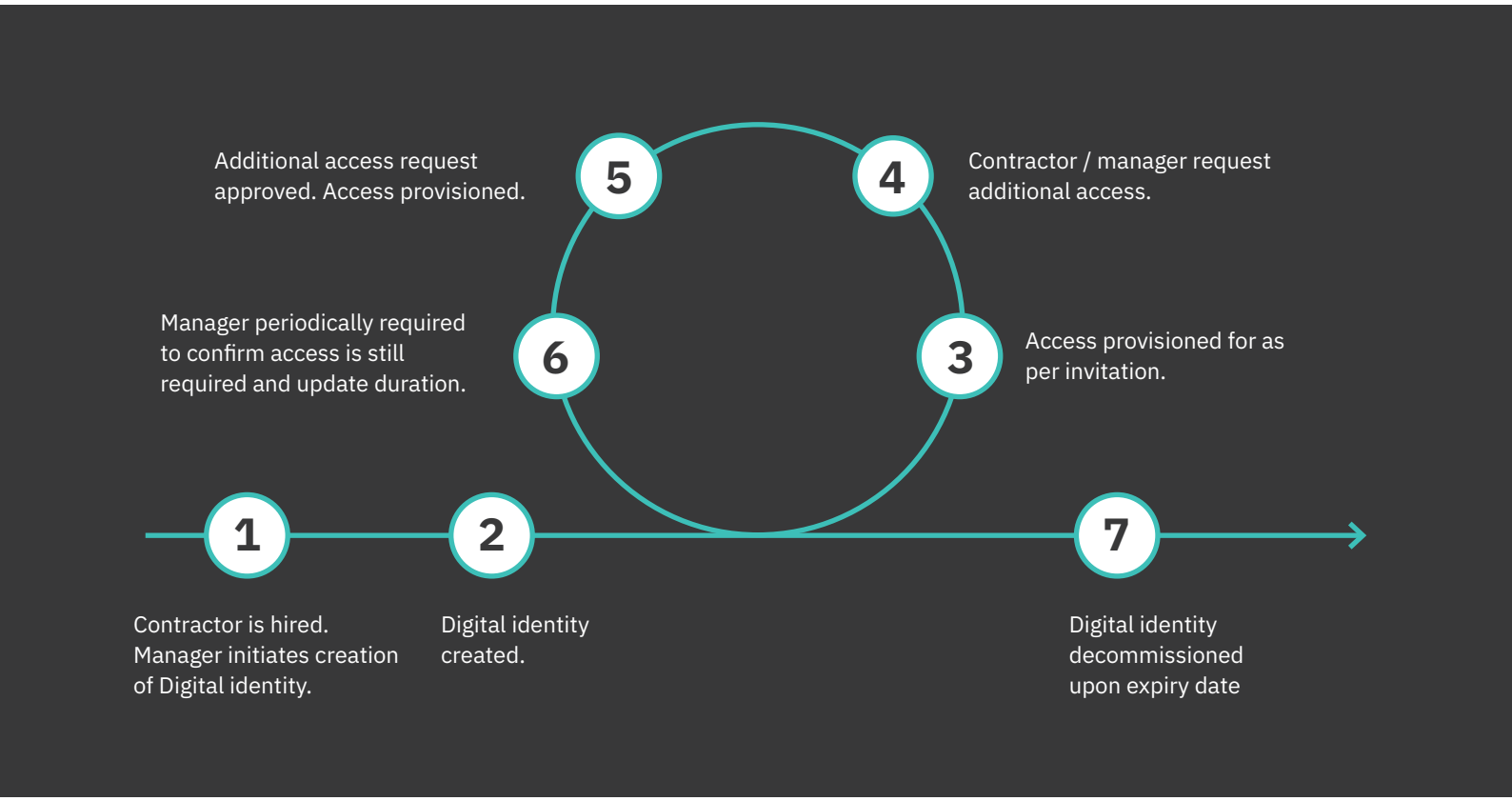
During the 'update' phase of the lifecycle, the process is the same as for staff. Access to applications and systems are automatically provisioned, either driven by information provided during the creation process, or by a request and approval workflow.

As for staff, certification of the identity is required however for contractors, this may well take place more frequently e.g. monthly. This is because often the organisation may not hold a contractual end date for contractors (as they may do for staff) and the end date may be indeterminate in any case e.g. if linked to an ongoing project which is experiencing delays.

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

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

Fig. 2. The contractor lifecycle



The B2B lifecycle

The B2B (Business-to-business) lifecycle refers to users from a third party that need to have access to one or more of the organisation's applications or services. Common scenarios include supply chain, distribution networks or distributed workforces.

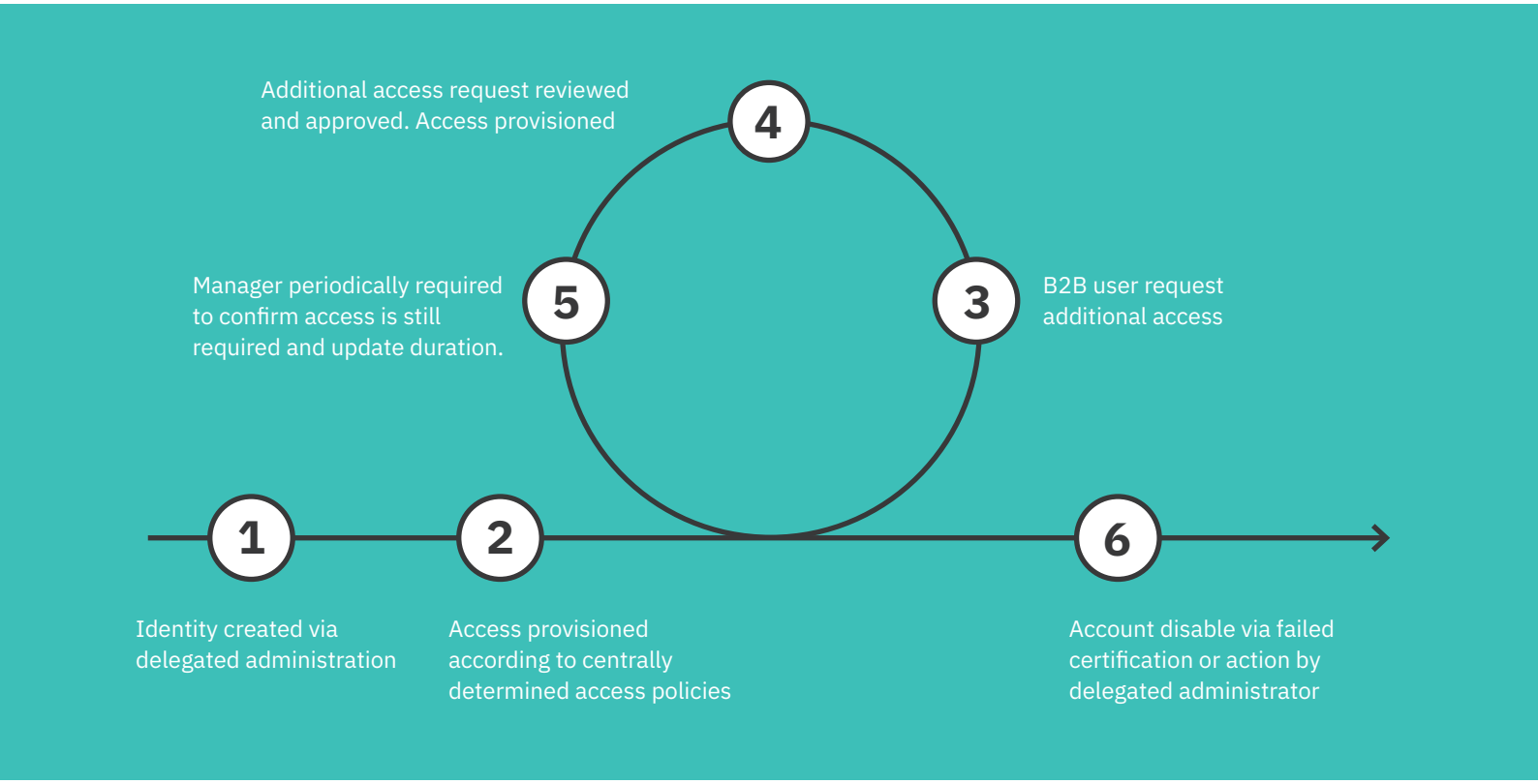
Managing identities for external organisations can be burdensome for the organisation, creating a lot of inefficient manual work for the IT or HR department. Therefore, a key driver for the B2B lifecycle is delegation – or the ability to 'delegate' administration of identities to the external organisations themselves. However, in so doing, it is equally important to ensure that there are tight, centrally controlled access and governance policies ensuring that identities created via delegation are managed properly in line with compliance requirements.

The B2B lifecycle is typically initiated by a delegated administrator at the external organisation, via an online form or invitation process. There may be a requirement for any identities created in this manner to go through an approval process. As for the contractor flow, the initiation of the lifecycle is not controlled by an authoritative source.

The update phase of the lifecycle is similar to contractors and staff – with access to applications and entitlements being controlled either by the delegated administrator or via self-service and an approvals workflow. However, given that the users are from a third-party, it is important that the access and self-service policies are controllable to ensure that no access may be granted to sensitive applications or data in error. As there is no authoritative source, self-service features are also essential for maintenance of identity attributes such as email address or phone number.

Certification of B2B identities is crucial – as there is no authoritative sources to drive date based decommissioning of the identity. Also, the risk associated with identities being left active inappropriately are high in a B2B scenario – consider the situation where a user from one supply chain organisation leaves and moves to a competitor, whilst retaining access via their previous identity. Such a scenario sets up potentially difficult situation with regard to commercial liability. Therefore, micro-certification (certification on an identity basis, e.g. every month) is essential, potentially bolstered by regular certification campaigns. Such certification processes ensure that accounts are properly decommissioned when no longer required, in the absence of an authoritative source of data.

Fig. 3. The B2B lifecycle



The customer lifecycle

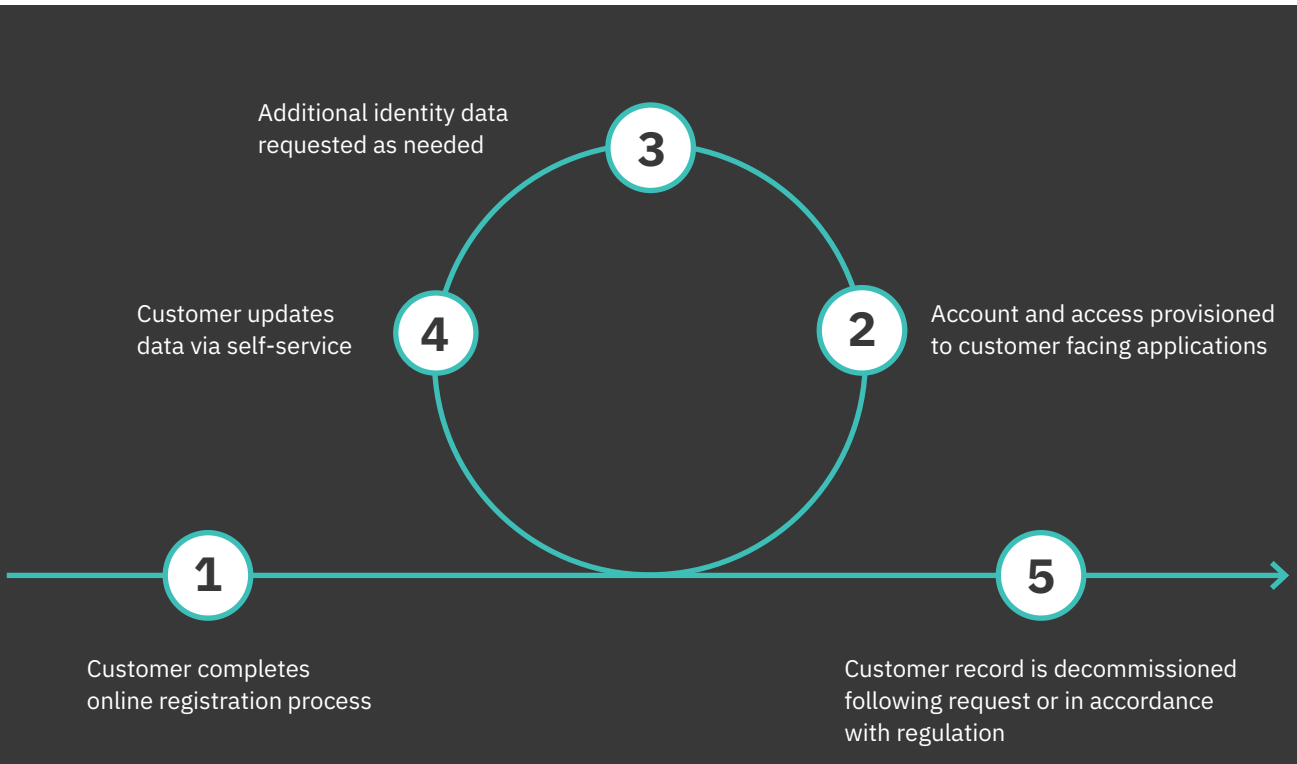
The customer lifecycle is quite different from staff, contractor and B2B lifecycles. Typically, the relationship with the enterprise is initiated by the customer via a self-registration flow. This may take place as part of an online purchase, or via an online registration form on the website. In most cases, the organisation will hold no data regarding the customer prior to the registration process.

As there is a focus on ease of use and user experience, it is common to reduce the amount of friction associated with customer registration as much as possible – so it may be desirable to minimise the amount of data requested about the individual at first touch to encourage potential customers to complete the registration process.

The update part of the lifecycle is likely to take two forms. Firstly, as a customer moves towards a purchase, it will be necessary, and desirable, to collect more information about the customer (e.g. billing and payment details). Part of the update process may then include an ability to request additional data over time. Secondly, self-service is extremely important for customers – especially the ability to help themselves with typical technical problems (such as forgotten passwords) or to update their contact information. A self-service portal therefore becomes a crucial component of the IGA platform.

In many cases, there will not be a defined end to a customer relationship, and therefore no automated decommissioning process. The delete phase of the lifecycle is therefore likely to be driven by other factors such as commercial or regulatory. For example, in Europe, GDPR governs retention of customer data, in particular Personally Identifiable Information (PII). This also includes the right for an individual to request that their data is removed – so it is important that the IGA platform provides for this, often via an API.

Fig. 4. The customer 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 summarises the key characteristics of various flows, showing the core requirements of each lifecycle.

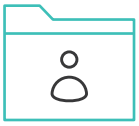
Fig. 5. Comparison of different identity lifecycles

Driven by authoritative sources	X			
Delegated administration		X	X	
Invitation		X	X	
Self registration		X	X	X
New account approvals		X	X	
Certification Campaigns	X	X	X	
Micro-certification		X	X	
Identity roles	X	X	X	X
Time-based events	X	X	X	
Access requests	X	X	X	X
Self-service	X	X	X	X
Profile management	X	X	X	X

Managing multiple identity lifecycles with ideiio

ideiio is an Identity Governance and Administration platform, providing both automation of the joiners/movers/leavers process alongside built in identity governance workflows, which help organisations to ensure that all their users have the right access to applications and data.

ideiio provides built in functionality to support all the identity lifecycles described above and enables organisations to flexibly manage the identity lifecycle for all their constituent users in a single identity management platform.

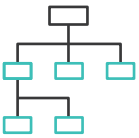


Provisioning driven by the authoritative source(s)

ideiio provides full support for provisioning of identities and access driven by one or more external authoritative sources, such as the HR system.

ideiio can interface with any external system via the ideiio Bridge module, which provides JDBC, LDAP and text interfaces, alongside connectors for common cloud platforms such as Office365 and Google Apps. The ideiio Bridge provides the flexibility to build custom modules, for example to interface with a custom user management API. Alternatively, as a standards-based platform, ideiio can communicate natively with any application supporting the SCIM protocol for provisioning.

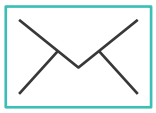
This approach means that the entire identity lifecycle can be automated from cradle to grave, to support the staff lifecycle. As multiple authoritative sources can be incorporated, this also means that organisations with multiple HR systems, or universities with an authoritative Student Records System can also be supported.



Delegated administration

ideiio provides one click delegated administration, allowing a portion of the system to be delegated to an external organisation or department, providing full support for the B2B lifecycle, as well as for federated or collegiate business models.

Delegated administrators can assume full control of the identity lifecycle for their users, with no visibility of any other identities within the system – subject always to the access and governance policies set by the central ideiio administrators.



Invitations

ideiio allows for administrators or managers to send invitations via email to onboard new users - this is ideal for the contractor lifecycle.

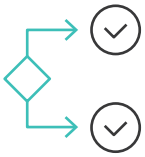
The system allows for access rules to be determined in advance in accordance with access policies; the digital identity and access are provisioned automatically once the new user responds and completes the invitation process.

Self-registration

ideiio allows unlimited self-service forms to be configured, allowing external users to request an account with the organisation – providing support for the contractor and customer lifecycles.

The forms, which can be branded in line with organisational branding guidelines and incorporated into an internet or intranet site, have the following features:

- Customisable form, allowing the organisation to choose which fields to include without any need for custom development
- Workflow driven, with requests routed to appropriate administrators from across the business to approve requests, depending on the role requested
- Incorporates Captcha and email verification to provide protection against bots



Approvals workflows

ideiio provides a comprehensive workflow engine, which provides workflows to govern many core identity events, including approvals for new identities.

Requests for new accounts, applications or roles can be routed to the relevant individuals or groups for approval. The request must be reviewed and approved before any automated provisioning takes place.

Certification Campaigns

ideiio provides identity certification campaigns, essential for the staff, contractor and B2B lifecycles. Campaigns allow access to a selection of applications to be reviewed on a regular basis by the relevant application owner or manager. In a fully automated system, this allows for a human to be injected into the process to make sure that there are no issues which may have been caused by, for example, data entry mistakes leading to individuals having inappropriate access. Where such anomalies are detected, ideiio provides the tools to remediate the anomaly in real time, for example by disabling the identity or removing the offending access.

Micro-certification

Micro-certification is the ability to perform certification on a per-identity basis, rather than as part of a campaign. Typically micro-certification is performed at regular intervals driven by an individual's start date.

Micro-certification intervals may be configured within ideiio, which determines when managers will be required via workflow to certify that individuals still require their access; if the identity is not certified, then access is automatically removed ensuring that there is no build up of accounts with inappropriate access.

Identity roles

The ability to map access to functional roles is an essential element of the staff lifecycle. ideiio provides a highly flexible, three-tiered role-based access control model.

Birth right resources are applications and services which are common to an entire category of users – for example all staff receive an email account. These resources will be provisioned to users of that category regardless of their functional role.

Identity roles relate to functional, or job roles. Individuals assigned to these roles will be provisioned with one or more applications which are relevant to that role – for example sales executives will be provisioned access to the CRM system.

Finally, a catalogue of self-service applications can be configured. These are applications which can be requested and/or added by an individual of their manager.

For all types of application, ideiio allows for entitlements to be managed. Entitlements represent permissions within an application being managed by ideiio, and can be controlled as part of the role model. For example, a role of 'Financial Controller' could be created to give access to the Finance System generally, and to the 'Accounts Payable' permission (or entitlement) within the Finance System.

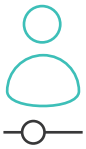
Time-based events

ideiio provides the ability for core identity events, such as provisioning or decommissioning an identity, to take place in the future on a given date. A common use for this is 'staged offboarding'.

Access requests

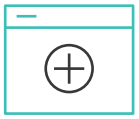
Self-service access request is fundamental to all the identity lifecycles. The ability for end users to help themselves saves time and effort for the organisation while dramatically improving the experience and productivity for end users.

ideiio includes with the Identity Portal, which is a web-based interface which allows end users to review their access, and to request additional applications and or roles. Requests are routed to the relevant manager or administrator for approval.



Profile management

ideiio allows users to manage their own identity attributes through the Identity Portal. The administrator can specify which attributes are made available for self-service.



Self-service

In addition to access requests, the Identity Portal also allows for users to add applications without the need for approval workflows. This could be used for non-sensitive applications within the staff lifecycle, or to allow customers to add additional applications or features as part of the customer lifecycle.

Identity Governance and Administration Maturity Model

Ad-hoc

- Not driven by authoritative data
- No automation of provisioning to connected applications
- No defined RBAC model
- Driven by spreadsheets and/or helpdesk tickets
- No governance (approval workflows or certification)
- No automated disablement of accounts

Basic

- Driven by authoritative data, but not synchronised
- Semi-automated provisioning via ITSM workflow for core applications
- Limited role and access rules
- Certification via spreadsheets or other paper-based system
- Semi-automated disabling of access via ITSM workflow

Developing

- Identity lifecycle driven by authoritative data
- Automatic sync of identity data from the authoritative source
- Automated provisioning to core applications
- Semi-automated provisioning via ITSM for all non-core applications
- Defined RBAC model
- Approvals workflows for core applications
- Automated disablement of access for core applications

Advanced

- Automated provisioning to all applications
- Full coverage across cloud and legacy, on-premise applications
- Self-service capabilities for end-users
- Approvals workflows for on-demand access requests
- Certification campaigns
- Micro-certification for external users
- Forensic audit trail
- Support for multiple lifecycles and user types
- Access and governance reporting and analytics

Conclusion

The modern enterprise interacts digitally with many different types of individuals – for example staff, contractors, partners or customers. For each different type of user, there are different characteristics of the relationship with the organisation which mean the relationship needs to be managed in a specific way.

These differences can be expressed by the identity lifecycle associated with each user. The identity lifecycle refers to all of the activities that needs to take place to manage an individual's accounts and access permissions across all applications that they need in order to do their job – essentially this means automation of all activities to do with creation, updating and deletion of accounts and access as the individual's association with the organisation changes over time.

The differences between lifecycles are nuanced yet significant. For example, the staff lifecycle is typically driven by data in an authoritative source such as the HR system. By contrast, there is no such authoritative source for contractors or partners, meaning that the ability to provide self-service and delegated governance features are essential in order to keep on top of things.

Identity Governance and Administration platforms exist to provide companies with the tools required to model, automate and govern all of these activities, ensuring that the right people have the right access to the right systems at the right time, whilst also providing the tools to prove this to support compliance requirements.

To be effective, an IGA platform needs to have the flexibility and features to cater to the different types of identity lifecycle that the organisation needs to manage. This includes a flexible RBAC model, support for coarse and fine grained authorisation, integration with multiple authoritative sources, self service and access requests and delegated identity governance.

ideiio is an Identity Governance and Administration platform, providing both automation of the joiners/movers/leavers process alongside built in identity governance workflows ensuring that organisations 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 organisations to flexibly manage the identity lifecycle for all their constituent users in a single identity management platform.

Find out more https://www.ideiio.com

Download the data sheet
https://www.ideiio.com/files/ideiio-datasheet-UK-v7.pdf

Getting started

Sign up for your free tenancy and experience the ideiio online demo
https://www.ideiio.com/#popup-try-ideiio

Glossary of terms

ideiio

ideiio is an Identity Governance and Administration (IGA) system that provides a platform delivering identity lifecycle management in an intuitive way. ideiio is built up of components such as ideiio core, identity bridge, identity portal and the governance portal.

Identity Governance and Administration

Identity Governance and Administration (IGA) can be described as a framework that encompasses policies relating to the management of identities within an organisation. These policies can be based upon industry standard practices or legally required government standards.

Identity

A digital record that represents a person within an organisation which records the attributes that make a person unique.

Self service access request

The process by which an identity can request access to additional systems through an online application catalogue.

Resource

Resources can be applications, Active Directory group memberships, hardware or user accounts for applications that people within your organisation will require for their job.

Birthright

Birthright assignments mean access which is granted to particular group of users, regardless of their functional roles. For example, we might say that all staff users in the US office are granted an Office 365 account, regardless of their job. In this case, Office 365 would be a birthright assignment for US staff.

Entitlement

Entitlements are specific permissions within an application that when assigned to a person, can grant them elevated privileges within the application or used to restrict what actions the person can perform within the application. For example, a person can be granted an ‘admin’ entitlement allowing them to perform elevated actions within that application, or a person could be granted a ‘default’ entitlement.

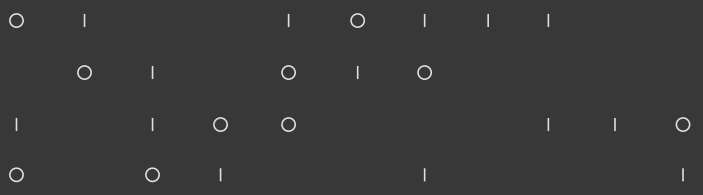
Coarse-grained

Granting a person initial access to a resource based on a role or category.

Fine-grained

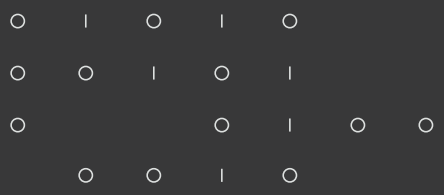
Granting a person specific access to an application via an entitlement, e.g. ‘admin access’ or ‘default access’.

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 3EQ, UK

t. +44 (0)161 204 7788

North & Latin America

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

t. +1 719 453 1067