Introduction to Identity - Part 1: Admin-time (v2)

By Ian Glazer, edited by Espen Bago

To comment on this article, please visit our GitHub repository and submit an issue.

Introduction: How to Approach Identity and IAM

Digital identity is a big topic; it touches every aspect of an enterprise's technical systems and services. This article is not going to offer a taxonomy of identity. Instead, it supports the idea that every individual and organization will likely approach digital identity from a different perspective and level of understanding, given their specific (yet perfectly valid) needs for their local identity system or service.

Identity is an often-debated term. Long-time practitioners and new members of the industry alike struggle with what "identity" means. This article suggests there is not a one-size-fits-all, definitive definition of identity. Instead, it encourages the reader to consider their own local context and adapt the rough definitions here to fit their organization.

This article takes a contextual approach, showing some possible ways of dividing up the IAM world and offering some examples of usage in context. Keep in mind that IAM is not just about technology. It is about the profession itself and us as practitioners.

Terminology

Joiner/Mover/Leaver: The joiner/mover/leaver lifecycle of an employee identity considers three stages in the life cycle: joining the organization, moving within the organization, and leaving the organization.

Sources of "Truth" - where authoritative data about individuals live.

Identity Governance and Administration - a discipline that focuses on identity life cycle management and access control from an administrative perspective.

Privileged Account Management - focusing on special control for risky high-level access. Privileged Account Management (PAM) is a mechanism for getting those special accounts under control.

Identity Proofing - accruing evidence to support “who this is.” Identity proofing is the last, but not the least, important part of this admin-time section. This is the process of collecting and verifying information about a person for the purpose of providing an account or a corresponding credential. This is typically performed before an account is created or the credential is issued, or a special privilege is granted.

User Provisioning and Lifecycle Management - how user records get where they need to be but only as long as they are needed

Entitlement Management – the business process to provision access

Role Management - a way to group access rules to make them more manageable

Role-Based Access Control (RBAC) - the use of roles at run-time; a way to govern who gets access to what through the use of roles.

Access Certification – the business process to verify that access rights are correct

Entitlement Management – Cataloging and managing all the accesses an account may have.

Access Certification - Certification is the ongoing review of who has which accesses

Identity analytics and intelligence mean looking at entitlement data, looking at the assignment of that, and trying to figure out and define what risk looks like. IdA provides a risk-based approach for managing system identities and access, with the intention of centralizing governance, visibility, and reporting for access-based risk.

Constituencies - who is it that we serve?

It is easy to lose the forest for the trees in the world of IAM, as there are so many little bits, nuances, abbreviations, and random factoids. Thinking about the ultimate stakeholder for whom the identity work is being done is one way to keep your focus on the big picture.

There are a variety of different constituencies that we serve as identity professionals, which means a variety of different technologies are needed to help them. These groups may include the traditional employee or the more complex groups such as customers, non-paid employees, contractors, and those not within the usual confines of an organization.

Whether that constituency covers employees, business partners, citizens, or students, in everything you do as an identity professional, you should keep the individual’s experience in mind. Holding the individual in mind grants more context and a broader view. This approach helps you to realize that “Hey, the reason why I am doing this automated

provisioning project is that we're about to hire 5000 new people, and we've got to make them productive on their first day of work."

Business-to-Employee (B2E): Making Employees Productive

For employees and contractors, the primary concern is productivity. The business wants their staff to be productive on day one and want their access removed immediately on separation. The mission here is to get the right access to the right people at the right place at the right time. That's what identity professionals are trying to do: get the appropriate access to people so they can be productive.

More often than not, the Human Resources (HR) department is in charge of employee data, and the HR system is the source of truth. Challenges with this include:

- Potential data integrity issues
- The organization may have multiple HR systems.
- Other non-employee data may (or may not!) reside in this HR system.

Regardless of the challenges involved, this is most typically our source of truth because if someone shows up in the HR system, they are going to get paid, so we need to make them productive; that's a very practical source of truth.

If there is one quote to think about with employee identity, it is "Who has access to what?" It is about making sure that the right people have access to the right stuff. The governing lifecycle, in this case, is the one known as "Joiner/Mover/Leaver":

- People **join** an organization.
- Their roles change as they **move** within the organization.
- Eventually, they **leave** an organization.

The HR system (or systems) acts as a source of truth for employee lifecycle events and related data, such as role or job codes.

Although contractors have similar identity and access-related needs, they may not share the same sources of truth. There may be instances where the HR system does not include the contractor population. Finding a singular source of truth for a contractor can be a real challenge in many enterprises. Some use their procurement system, some use bespoke systems, some use spreadsheets, and some even use their user account provisioning system. For temporary or seasonal workers, it may be most efficient to use a social media identity provider to onboard these types of short-term staff, provided that the organization can obtain the necessary level of assurance.

Business-to-Business (B2B): Connecting to Partners

The next constituency is our business partners. In every industry, we need to connect with our business partners. This connection is really about making sure that members of your supply (or value) chain can interact with you: You are giving them apps to use to work with you, but where do the identity records for these people come from?

Ideally, partners arrive with the identity bits provided by their organization. In that case, we are dealing with the business partner's system of record, likely their HR system, and you are one degree removed from it. This distance often means that you have delegated the administration of doing life cycle management. However, in high-risk applications, the owner of the application may want to control the access rather than trusting the business partner.

From an IAM perspective, B2B and B2E are very similar. The key difference is the source of truth. Often the enterprise doesn't have a system that specifically tracks individuals who are employees of their business partners. Instead, they delegate the management of those people to other systems, either in their own enterprise or in the partner's organization. More often than not, the IAM systems become a de facto source of truth for individual partner identities.

Business-to-Consumer (B2C): Digitally Engage

Last but not least is Business-to-Consumers (B2C). B2C is about bringing whatever the awesome thing is that your organization does or sells to the people. When you talk to the people in your business building the consumer-facing service, you'll often hear them describe the way a consumer interacts like this: "The person is going to do this, and then the person is going to do this." And an identity professional would ask questions like "How did that person get there?" and the answer would be, "Well, yeah, they logged in." And suddenly, you realize that the people building the service have no idea what we as identity professionals do at all. This lack of understanding is an amazing opportunity to make that awesome thing that your organization does get to the right people. That is your mission.

But in this world, the life cycles are different. It is about the individual, the citizen, the consumer. In many ways, they are in control of the life cycle, not you, and you have to be able to accommodate that.

The mission of the business is, "I want to deliver an awesome experience." No one is in the business of just giving people an account and calling it a day. In a B2C setting, you cannot say, "Great! You can log in; I am done here." No, that is just the beginning of the relationship. There is a focus on the customer experience, and we as identity professionals are helping deliver that experience. We are a critical onramp for it.

B2C use cases illustrate that we, as identity professionals, are not alone in our enterprises. We cannot get our jobs done without our peers in security and privacy. There are three legs

in this stool to make it work. For privacy, identity provides operational controls, especially in the context of access to data. And for security, identity offers a valuable framework. We put the "who" in the "who the heck is on my network" kind of questions. So if you are working in a B2C (or B2B) setting, and you have not met your peers in the privacy and the security team, go seek them out. They have valuable tools that you can help enrich and that can help you as well.

Technologies Involved - Admin-time vs. Run-time

Having established the constituencies we serve, it is time to look at some of the technologies we use to do that. One approach among many valid ways of sorting out the various technologies and terms is to split the world into administrative (or admin-time) and run-time discussions.

Essentially, the technologies and disciplines used to set things up are on the admin-time side, and the things that are being used when the user is logging in or going through a forgot-password process are on the run-time side.

Admin-time Technologies

The three main areas within the admin-time sphere are:

- Sources of "Truth" - where authoritative data about individuals live.
- Identity Governance and Administration - a discipline that is really about life cycle management and access control from an administrative perspective.
- Identity Analytics and Intelligence - of particular interest to large firms to help assure access is correct.

Two additional areas are also admin-time but do not always fit in the same bucket. Some industry analysts like to add these categories:

- Privileged Account Management - focusing on special control for risky high-level access.
- Identity Proofing - accruing evidence to support "who this is."

Sources of "Truth"

How do I know who someone is? That may be too difficult a question to answer from both a metaphysical and practical perspective. We can instead rephrase it to: "How can I find reasonably good, authoritative records about people? I need to send their paycheck somewhere." Or, "I need the shipping address of my business partner. How do I find this data?"[i]

For employees, the answer tends to be HR. For partners, it tends to be that delegated admin one step removed from their HR system. And in consumer settings, things get more

complicated. In low-risk areas, the answer is the individual. They are the authoritative source for much of the information you will use. For convenience, this may come from a social media profile, for instance. But in higher risk areas such as financial or medical, the answer may include authoritative sources such as their institution of higher learning or their local government. In an educational setting, a student information system may serve as a source of truth for students.

Data quality is an essential element here. We depend on data for doing things like ensuring people have the right access. But the data from the source of truth is not always reliable, so we may have to operate under the assumption that data quality issues may exist.

Identity Governance and Administration

These are the tools that manage who has access to what. They are the tools that rely on a source of truth (the who) to govern entitlements (the access) in target systems (the what) via connectors.

Identity Governance and Administration (IGA) tools are traditionally more focused on employees, contractors, or students. These tools can often be thought of as more traditional, enterprise-centric tools related to ERP systems.

This area is considerably larger than the other five areas of the admin-time sphere, and our coverage here will focus on the following subsections of it:

- User Provisioning and Lifecycle Management - how user records get where they need to be but only as long as they are needed
- Entitlement Management – the business process to provision access
- Role Management - a way to group access rules to make them more manageable
- Role-Based Access Control (RBAC) - the use of roles at run-time
- Access Certification – the business process to verify that access rights are correct

User Provisioning and Lifecycle Management

User provisioning is the mechanism that helps create, maintain, and eventually remove user accounts in target systems. This mechanism can listen to joiner/mover/leaver events from sources of truth (for example, a connector to the HR system listening for events such as the addition of a new hire). That event then triggers the provisioning system to evaluate the user through business rules in order to undertake required actions, such as create a new user account in Active Directory. The mechanism also has rules describing what those triggered actions are, such as to start setting up access based on some attributes from the new hire data. That typically means assigning entitlements, which can be something that requires approval. For basic entitlements like “birthright” access, we may not need approval. For example, all employees should get access to the productivity suite and email,

none of which require approval. If, on the other hand, someone wants to obtain access to the mainframe as a sysadmin, that is going to take some approval. You will have both types — access requiring explicit approval as well as access that does not — in almost all organizations.

A common mistake is to try to automate everything. Avoid this! There are hundreds, if not thousands, of systems and services in your enterprise. Trying to automate provisioning to all of that is just diminishing returns. So what then should be automated? The candidates to look for are the systems with the largest user populations or the highest turnover in those systems. Automation is essential for high-volume or high-velocity systems. Other candidates are systems with too many requests for your helpdesk team to manage, or the ones so sensitive that you want to lock down the rules of who gets access to it. Those make sense to automate.

Day one access systems are excellent candidates for automation. Partly because it is to some extent non-controversial; you get email, you get productivity, you get inside the employee portal, maybe you get VPN. Creating these user accounts has to happen for all new employees and represents a large administrative burden ripe for automation.

After day one onboarding and for the vast number of remaining systems, you are going to provision additional access manually. This means either people will ask for access and/or you will manually create the account (often because you do not need to do it very often.) And in some cases, that system that you want to create an account in exists away from your sphere of direct influence; you will not have a connector to the system. For such systems, the only way you can get to it is by opening up a support ticket, and a human will have to directly access the system to create or change the user account. These typically do not need to be automated.

Lastly, provisioning systems are often involved in setting up passwords. This involvement means that provisioning systems often need to have aggregate password content rules. That exposes all sorts of challenges because different systems can have radically different internal rules and password capabilities. For example, you may have a password content rule that mandates the inclusion of a special character. Because of system proclivities, a person could provide a password with a special character that the Oracle database could not accept, but Active Directory could. User provisioning (or password management) systems have to deal with these potential problems as gracefully as possible.

Entitlement Management

Now we have a source of truth and users flow into a data repository, and that triggers our user provisioning systems and starts creating users in our target applications or services. But it is not enough just to create a user account; we also have to know what that account can do. This set of actions is what we call entitlement management. Entitlement management can get really detailed really fast because the total of all the little privileges

that govern what a user can do in a system can be extremely numerous. It is not unheard of to have hundreds, if not thousands, of individual privileges in a system. Those privileges are often aggregated into user groups or roles, which can also become quite numerous. It is like grains of sand on the beach, which is why we try to aggregate them together. Imagine you have three employees, one system, and four privileges in it: Create Purchase Order (PO), Update PO, Read PO, and Delete PO. Connecting each person to the right collection of privileges is possible, but it becomes unmanageable very quickly.

That's where layers of abstraction come in: We put this thing in between the user and the privileges called an entitlement. We say, "This allows you to manage purchase orders." And it is these things that the provisioning system hands out, instead of the detailed privileges themselves, because there are way too many discrete privileges to keep track of. We abstract the details and instead say, "Here's an ability," or "Here's something associated with your job responsibility." Unfortunately, those discrete, detailed privileges still need to exist in order to allow the level of granularity an organization's business processes require, and to provide the level of instruction to the system that can be coded into the environment.

Entitlement management means cataloging all the accesses a person can have, which can be a massive undertaking. For example, a medium-sized bank may have ten major systems (but often a lot more), which means you may have thousands upon thousands of privileges, which are aggregated into a thousand or so entitlements. You then need to figure out how to map that to the business needs. Entitlement management is this cataloging process.

Ideally, you are bundling privileges together into sets that make some semblance of sense for people and the organization. For example, imagine that you want to gather all the entitlements together that someone who works in purchasing would need. Or that you want to make sure you have put together the relevant entitlements that someone who is a business partner - at the gold tier but not the silver tier - has access to. This level of efficiency is what you and your identity colleagues are working towards to make access to enterprise resources manageable.

It also tends to be mandatory work if you're ever going to do Segregation of Duty[ii] analysis, for example for Sarbanes-Oxley (SOX)[iii] compliance or General Data Protection Regulation (GDPR)[iv] compliance requirements, where we have to identify combinations of accesses that together are dangerous. For example, people who can authorize payments to partners should not be able to create a fraudulent partner and pay them.

Role Management

But even when we have worked these entitlements down to a level where they are manageable entities in themselves, using them effectively will be very challenging. The answer to that challenge for many, though not all, organizations is to try to do something called Role Management. You may have heard of it as Role-Based Access Control (RBAC).

The essence of it is as follows: in some organizations, job functions are very regular. Regular job functions are most typically found in hierarchical organizations. On the other end of the scale, this works quite poorly in matrixed organizations; that is because it is hard to pinpoint, for example, the three top job responsibilities, as they are always shifting.

Role management can be useful for saying, “These types of job responsibilities need this kind of access, so let’s call that thing a Role.” Additionally, sometimes you have this thing called a technical role, which is saying, “Here are the low-level bits you’re going to need to do your job,” and it becomes a handy bundle to assign to people. Imagine roles as a grouping to which you might provide access in a common way. You should only create roles if you are going to provision or control access to a group differently. At the highest level, you could only have a handful of roles, and you should review them regularly as your organization evolves.

Role-Based Access Control

RBAC is just a way to govern who gets access to what through the use of roles. There is no need to overthink it. It works great in regular, hierarchical, homogeneous organizations. Not surprisingly, it works really well for places like the US Department of Defense. It does not work great for the 150-person start-up; do not try to do that.

When overthinking RBAC, or over time in general, you can get what we call a “role explosion,” where you have more roles than you have people. Some of the salty veterans say, “oh yeah, I survived that. They told me that was a good idea. It was a horrible idea.” Try to avoid this situation; it rarely ends well.

Access Certification

At this point, people have access. They are productive on day one. They are productive on day two. On day three, they start to become a privileged threat because they have too *much* access. And the best way to get more and more capabilities in an enterprise is to simply change jobs. You go from doing this job to another job, and if your business rules didn’t explicitly prevent the continuation of access, experience shows that you do not lose your old access, you just keep it on top of new accesses.

Another instance of accumulating accesses is when you onboard someone new, with the dreaded situation of “Whose access should we model you after.” Anyone who has gone through any kind of IT security audit knows how horrifying an audit can be. A common answer to the question of whom to model a set of new accesses to give to a new employee is their boss. The boss is likely to be the biggest source of access violation around because they have accreted access over years. They are a horrible person to emulate for this purpose, from a risk management perspective.

Certification is the ongoing review of who has which accesses, a process that became popular with the introduction of the Sarbanes Oxley law (SOX) in the United States. It is a great tool to prevent people from keeping access they no longer need. An auditor might say that this should be done quarterly, something that quickly becomes very fatiguing. Better methods may be to trigger reviews based on changes to entitlements, changes to overall user risk, or to try to detect if someone deviates from a norm. In other words, we want to certify whether, if compared to a set of peers, you are an outlier. We want to figure out why that is. It is a powerful way to make sure you don't have issues with the access and entitlements that you've assigned in a non-automated fashion.

All of the mentioned elements add up to a lot of data flowing around. With all the users, times all the systems, times all the entitlements, times all the roles, times all the privileges, the total is staggering. How can we make sense of it all?

Identity Analytics

One of the ways is through identity analytics (IdA) and intelligence, which is more than just reporting on "Who has access to what."

Identity analytics and intelligence mean looking at entitlement data, looking at the assignment of that, and trying to figure out and define what risk looks like. What does a normal user look like? Compared to that, what does a heavily privileged user look like? What does the model of a system administrator look like compared to developers, someone working in finance, or someone working in the field sales organization?

The goal is to find commonalities of outliers among user populations and to understand what access-related risk looks like in the organization. Other goals of IdA include being able to group commonly assigned entitlements together as candidate roles, to identify over-privileged users, to discover undocumented high privileged access rights assigned to regular, non-privileged accounts. IdA can also accurately measure and report on user, account, entitlement, application, departmental, and organizational risk posture.

IdA provides a risk-based approach for managing system identities and access, with the intention of centralizing governance, visibility, and reporting for access-based risk.

It uses dynamic risk scores and advanced analytics to determine the associated level of risk and to derive key indicators for automating account provisioning, de-provisioning, authentication, and privileged access management. This approach reduces the identity attack surface by identifying (for remediation) unnecessary, unused, and outlier access.

Another feature of this admin-time function of risk determination is that the indicators and data it produces can be integrated with, and used by, your run-time systems. For example, during the login process: If we know that a person is not particularly risky, then they might not need to be challenged for additional authentication factors. But if, on the other hand,

that person has a lot of privilege and power in the systems, and maybe they deviate from the norm in their job role, then they might need to provide additional verification. Run-time risk determination analysis such as this can be partly or fully automated, depending on the quality of the indicator data and the maturity of the organization using them.

Privileged Account Management

Some of the user accounts out there are special. Your sysadmin accounts, your root accounts, and so on. These accounts are not necessarily tied to people. But they are super privileged user accounts. We may have a whole team of people that have to act like the root administrator. Privileged Account Management (PAM) is a mechanism for getting those special accounts under control. You can essentially check them in and out as needed: "Hey, I need to go in and apply a zero-day patch, so I need to act like the root administrator for this," and the system will grant the relevant access for that purpose, after validating who the user is. It may also record the screen, so that as the user is performing their actions, what's going on is being logged. One use case for this could be when having a third-party service vendor who's going to come in and do maintenance on specialized pieces of equipment, where we need to have an audit log of the actions that they took. This log would be like the record function in privileged account management. Another important function is scrambling the password for these special accounts, so that no one retains the password to the root or sysadmin account after the job is done, such as the patch job in the example above.

Identity Proofing

Identity proofing is the last, but not the least, important part of this admin-time section. This is the process of collecting and verifying information about a person for the purpose of providing an account or a corresponding credential. This is typically performed before an account is created or the credential is issued, or a special privilege is granted. It also tends to be a lengthier process the first time we encounter a particular individual, as opposed to the secondary proofing required for purposes of account recovery.

The process is often found in regulated industries, such as in banking, with requirements for doing Know Your Customer (KYC) and anti-money laundering. These require government documents to be presented in some fashion, proved to be accurate and valid, and then associated with the individual. This is the proofing process.

Depending on the account or credential to be issued, there are different ways of doing proofing, many tied to government-issued identity. In contrast, others are based on what we call self-asserted.

In an enterprise setting, B2E, relating to employees, proofing is a very common process, involving background checks and showing documentation (for example, your passport or a driver's license) to get your job. For employees, we want to do this because this is how we

will get a new job. But for a B2B setting, it is a very different situation. How do we onboard a new business partner? In addition to making sure who that person is, we may need proof that this is the organization we want to work with and that *this* person is someone we want to work *within* that organization. These different criteria make for a very different kind of proofing process.

What about identity proofing in B2C use cases? How does one know and trust a new customer who makes a claim about themselves? Here it is a question of how much we need to care about that. There is a trade-off in the B2C world between velocity versus veracity. For some organizations and apps, the priority will be velocity - to get people registered quickly and into the app as fast as possible. The user journey is optimized for this. They'll have very limited access, and the threshold for user registration is very low.

For others, the priority is veracity, either because of the brand experience, because of the business they're in, because of what they want to deliver in terms of value, or related to the chance of fraud. In this case, the enterprise wants more verifiable data about the person. The enterprise determines it is important to have a higher level of assurance that the new customer is really the person they claim to be.

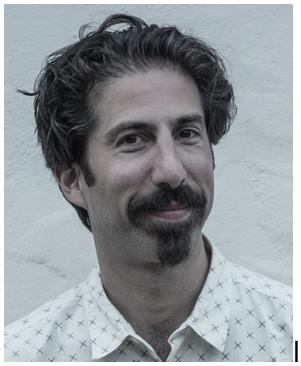
Conclusion

Digital identity, as we indicated at the beginning, is a big topic. We've touched on the constituencies IAM serves, the technologies involved, governance, analytics, privileged accounts, and identity proofing. Each of those topics can (and hopefully will, in future versions of the IDPro Body of Knowledge) fill out an entire chapter by itself.

The article offered the IAM practitioner a chance to understand some of the major considerations that will impact their systems and services; readers need to consider their own local context and adapt the rough definitions offered here to fit their own unique organization. A future article will dive into the concept of run-time technologies.

Author Bios

Ian Glazer



Ian Glazer is the Vice President for Identity Product Management at Salesforce. His responsibilities include leading the product management team, product strategy, and identity standards work. Prior to that, he was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where he oversaw the team's research. He is the founder and president of IDPro, the professional organization for digital identity management. He was also a founding member of the Management Council and Board of Directors for the US Identity Ecosystem Steering Group (IDESG). During his decade-plus time in the identity industry, he has co-authored a patent on federated user provisioning, co-authored the Service Provisioning Markup Language (SPML) Version 2 specification, contributed to the System for Cross-Domain Identity Management (SCIM) Version 2 specification, and is a noted blogger, speaker, and photographer of his socks.

Espen Bago

Espen Bago realized in 2002 that as system administrator, he'd been working in identity already for a while and decided from there to fully explore what this Identity thing was all about. He's been an independent Identity Advisor and coordinator to large enterprises for the last few years, but in 2021 became Identity Manager for the Norwegian Labour and Welfare Administration. As such, his goal is to make certain that identities – and the real persons this represents – are not forgotten when governments inevitably go all-in digital. He's also a founding member of IDPro and a member of the IDPro Body of Knowledge Committee and the IDPro Certification Committee.

Change Log

Date	Change

2021-06-30	Editorial updates; addition of a Terminology section; update to B2E section

[i] An organization does not always need to know "who" a person is to any level of specificity. They just need to know things like "is this the same person each time" or "is this account authorized to perform this action."

[ii] AICPA, “Segregation of Duties,” accessed on 11 January 2020, https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html

[iii] United States. 2002. *Sarbanes-Oxley Act of 2002,* [Washington, D.C.]: [U.S. G.P.O.], https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

[iv] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.