opentext™ | Cybersecurity

White Paper

NetIQ Identity Administration Needs Governance

Table of Contents

Abstract

Organizations have been trying to manage identity for many years. It began with a focus on identity provisioning, simply a function for IT to onboard new employees: “Larry is starting today in Sales. What does he need access to in order to get up and running?” Over time, this evolved into identity lifecycle management. It quickly became evident that it was difficult and costly to automate identity and access management across so many applications. As compliance regulations and policies were added to the mix, requiring least privilege and separation of duties, review and certification became an additional method of managing access. Enter the need for governance, and now the analysts have declared that the markets for both provisioning and governance have merged into “Identity Governance and Administration” (Gartner). This white paper explains how this happened, why it is needed, and how your organization can achieve governance as an integrated part of your identity management efforts.

Organizations have been trying to manage identity for many years. It began with a focus on identity provisioning, simply a function for IT to onboard new employees. Over time, this evolved into identity lifecycle management.

The Original Requirement

Somewhere, one day, an IT professional got tired of manually entering in all of a new user’s information over and over again to set them up with an identity in each system they needed access to. Users needed to be set up not only in the main identity directory, but also in all the other systems and applications they needed access to. It wasn’t uncommon for new users to wait days or even weeks to get the access credentials for all the systems they needed in order to do their jobs. During this time, IT was under enormous pressure to complete the task as quickly as possible so the employee wasn’t sitting idle, being paid to do a job they weren’t able to start. This not only affected operating expenses, but could also impact revenue, depending on the user’s role. This process was also very monotonous for the IT staff and took them away from other work they needed to do. At one point, an IT staff member stopped and thought, “There must be a way to automate this so I can speed up the process and not have to enter this person’s name over and over again in every system they need access to.”

Soon, tech companies began to develop user provisioning tools, many of which leveraged or connected to Microsoft’s Active Directory for this very purpose. These tools were designed to save time and make it easier for the IT staff to get new users up and running quickly, with access to the applications they needed to do their work. Everything worked great and there was much rejoicing—well, not quite.

The Evolution of Needs and Challenges

After IT teams began using automated provisioning tools, it helped to speed up access in some areas; however, new needs and challenges began to emerge—and they are still emerging today. While many issues have arisen, this paper focuses on three main themes: complexity, compliance, and security.

Complexity

One of the big issues in automating the identity management process was that with so many different systems, it became very complex very quickly, and it was difficult to get all of them "talk to each other." For example, organizations were able to connect a good portion of their systems and applications so that the IT team could create a new user and have it pushed out to several others, but there always seemed to be exceptions that still required manual efforts. And if you needed to make a change to one of the applications that was connected, it meant you likely needed to do a lot of work to the identity management tool you were using as well, in order to establish the new connection. Sometimes the tool didn't support the change and you had to do some custom work in order to get things to work. Then a new version would come out and you had to do it all over again and again and, well, you get the idea.

Compliance

It's no secret that an organization's most valuable asset is its data. But access to that data is based on an individual's (or entity's) identity within that organization. As more and more data breaches began to occur, new compliance regulations emerged, detailing specific policies about who could access what—or more importantly, who couldn't access certain things. These compliance regulations quickly put new pressures on the IT teams that worked on identity management within the organization. For starters, they needed to understand who had access to the specific applications in question but due to the complexity issue mentioned above, it wasn't as simple as running a report that easily listed the users. In fact, producing a report for the auditor could be a very labor-intensive task. Due to the nature of different identities in the various systems, a user might be listed as smith.john in one system, j_smith in another, and so on. So, even finding and then correlating the users was tricky.

And since there was no master set of rules to automatically check and ensure that no one had access that they shouldn't, and because not all of the systems were connected to that one master set of rules (if it even had existed), again it was left to the IT staff to manually scour all the different lists of users to see if any violations existed and then prove they had fixed any violations. This required the creation of a full-time position for larger organizations. Another factor is that IT teams had no way of knowing whether an end user should have the access. They simply had no visibility into that level of information.

Security

Security is very closely tied to compliance as well, but brings with it some additional challenges beyond simply adhering to compliance. One of the key security challenges that developed related to de-provisioning users when they left the company or changed roles. The approach relied on human action to remove access; many people took time to have their access removed, but in some cases, it simply never was. This presented a security risk in that an organization could be exposed to potential breach activity from a former employee. Consider as well that even if the employee's access was terminated, the IT department still didn't have a master list of everything the employee had access to for the same reasons mentioned above in complexity and compliance.

After IT teams began using automated provisioning tools, it helped to speed up access in some areas; however, new needs and challenges began to emerge—and they are still emerging today. While many issues have arisen, this paper focuses on three main themes:

- Complexity
- Compliance
- Security

Security is very closely tied to compliance as well, but brings with it some additional challenges beyond simply adhering to compliance. One of the key security challenges that developed related to de-provisioning users when they left the company or changed roles.

Another aspect of identity management security was passwords. Since end users had so many different identities, they had difficulty remembering their passwords, so most would just use the same one for everything. The problem with that is that if one login was exposed, someone potentially now had access to all the different applications.

External Users

As businesses and technology evolved, more staff began to work remotely and businesses also leveraged partners to outsource certain aspects of their duties. Whether it's a remote employee, a contractor, or a vendor performing a service, these workers must have access to the information they need in order to do their jobs.

This presented IT departments with the challenge of ensuring security while enabling productivity. A crucial facet of this access was ensuring that it was terminated in a timely manner once the access was no longer needed. Otherwise, the organization is leaving an access point open for potential exploit. Additionally, extra care needed to be taken from a security and authentication perspective because if a vendor who has access has lax security on their system, the organization risks getting exploited via that weak point. If there's a data breach, the auditors and customers whose information was stolen aren't going to give the organization a pass simply because it was a vendor's security protocols that initially failed. It's still the organization that's ultimately responsible at the end of the day. The reality is there are extreme difficulties in managing the rights and access of external entities because there is often no active record of their current relationship with the organization and whether it should be retained.

As we fast forward to the present, IT managers remain under extreme pressure to protect business-critical assets even while they have too few resources to defend an attack on a surface area that is expanding exponentially.

Current Approach and its Limitations

As we fast forward to the present, IT managers remain under extreme pressure to protect business-critical assets even while they have too few resources to defend an attack on a surface area that is expanding exponentially. There is no "silver bullet" that has worked for every application, in every company and in every scenario. So the current approach is really made up of a patchwork of various tools.

A majority of larger organizations are using some form of identity management solution and have connected as much as they can to it. They likely have also leveraged a single sign-on approach to deal with some of the issues we presented in the earlier sections and to address password concerns. From an identity management or administrative perspective—aside from the few applications they still have to manage separately—they have improved efficiency and might even have a request portal for the end users to request additional access.

However, what most organizations today are lacking is governance as it relates to their identity management. This is a very serious issue because without any oversight or recertification of existing access, how can you be sure you aren't exposing your organization to compliance violations or putting your data at risk of exposure? Without the governance component of identity administration, there are no checks and balances that involve the line of business side of the organization to determine if access is appropriate and warranted.

Pivoting the Approach

Realistically, your organization can't afford to start from scratch as if it's day one. It's a luxury you don't have. That said, there are things you can do to pivot your approach to begin to add in or augment the governance of your identity management. You should consider taking a strategic approach that balances risk and your business needs. You don't want to implement something so severe that it hampers your efforts to conduct regular business, but you also want to avoid something so lax that there is little protection from risk. In determining the solution you will implement, you must take into account its ability to account for these three factors.

Realistically, your organization can't afford to start from scratch as if it's day one. It's a luxury you don't have. That said, there are things you can do to pivot your approach to begin to add in or augment the governance of your identity management. In determining the solution you will implement, you must take into account its ability to account for these three factors:

- BYOD and the Proliferation of Devices
- Reduce the Attack Surface
- Digital Transformation

BYOD and the Proliferation of Devices
Does the solution account for mobile access, recognizing that many users access applications and data from their mobile devices? Can the solution take advantage of mobile so that line of business managers or end users can access the request or recertification solution on the road?

Reduce the Attack Surface
One of the goals in leveraging a governance solution is to reduce your risk factor. Will the solution be able to import the data from your existing systems to interpret potential exposure in a timely manner without requiring a great deal of customization? If you do not need to alter the data very much, your solution should be able to quickly highlight and provide decision support for some high-risk identities that you should look at first (for example, users with access to a higher than average number of applications, or those who access from a higher than normal number of IP addresses).

Digital Transformation
Investing in an identity governance solution is very important and, as described in some of the previous sections, infrastructures can be very complex. One reason for this complexity is the constant change in technology. Therefore, when determining a governance solution, you will want to look at considerations such as the solution's adaptability to connect to new cloud applications. The needs for identity governance don't change based on whether the application is on premises or in the cloud.

In an earlier section, we covered the challenges of external users. This comes into play here as well, but it's important to note that digital transformation has expanded what it means to be a "user." Organizations can now have devices, vehicles, and other forms of technology connecting to their network, so you need a solution that is able to build a relationship between these users, devices, and things to ensure that appropriate access is granted and governed on an on-going basis to account for changes. When evaluating available solutions, an important consideration is whether the data transferred between these "users" needs to be provided in a specific format or whether it's flexible. You will want your investment to be able to be leveraged into the future and not just for the needs of today.

The NetIQ by OpenText Governance Method

NetIQ by OpenText™ works as a partner with our customers on an approach that incorporates governance into the identity management and access request process. Your organization can leverage this approach to simplify, secure, and remove a lot of the burden on your staff. With over 5,300 customers worldwide, we have worked with organizations of numerous industries and sizes and have modelled an approach method on how to tackle identity governance and administration (IGA).

NetIQ by OpenText works as a partner with our customers on an approach that incorporates governance into the identity management and access request process. Your organization can leverage this approach to simplify, secure, and remove a lot of the burden on your staff.

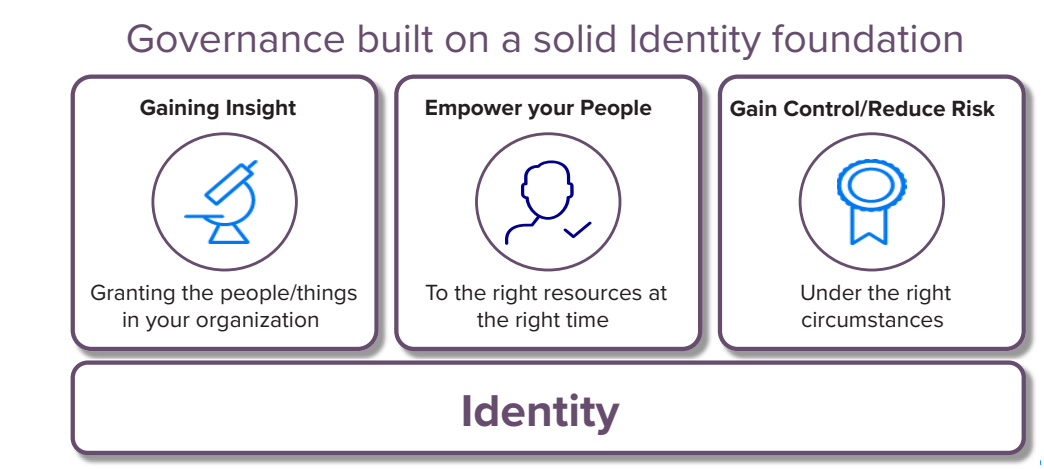

Figure 1. Governance built on a solid identify foundation

1. **Gain Insight**—identity discovery and mapping to establish a clear understanding and start building a foundation of what you have and what is needed by who.
2. **Empower Your People**—involve the business to make a real impact on the efficiency, responsiveness, and decision making; have new access requests and recertification go to the appropriate business owner while providing them with the information they need to make the proper decision.
3. **Gain Control/Reduce Risk**—implement your rules and policies with intuitive intelligence that identifies violations, notifies the appropriate people, and stops them from happening.

You'll note that the foundation for this method is based on Identity. It's all about having a central management solution that provides that single view of all the identities in your organization, enabling you to gain insight, empower your people, and gain control to reduce risk. The repository of identity information is really the foundation here and it's crucial that you get this part right, because the decisions will be based on the data contained within. NetIQ Identity Administration by OpenText and NetIQ Identity Governance by OpenText are two sides of the same coin, equal in importance.

Why Us, How Are We Different?

While many solutions on the market tackle either identity administration or governance, OpenText is different because we have an integrated approach to identity governance that leverages common components for a unified experience for both your users and your IT staff. This approach, as well as our experience, have several benefits to your organization.

Less Complexity and Fewer Services
Through integration, we're able to reduce the number of custom services you would typically need to purchase through other vendors to make their governance and identity solutions talk to each other. In terms of importing and interpreting data from your various applications, in most cases our IGA solution is able to read it as is—saving you conversion and rewrite services. And the user interface provides end users with decision support for an easier user experience.

Single Point of Contact
If you are relying on two (or more) different vendors to tackle this challenge and you have a technical support issue, you will need to make several calls. Additionally, you can sometimes encounter the blame game of one vendor telling you it's the other vendor's software that is causing the issue and vice versa. When you leverage the same vendor for both identity administration and governance, you have one company to call. We have no concern with blame. Instead, we concern ourselves only with finding the solution.

NetIQ by OpenText is different because we have an integrated approach to identity governance that leverages common components for a unified experience for both your users and your IT staff. This approach, as well as our experience, have several benefits to your organization:

- Less Complexity and Fewer Services
- Single Point of Contact
- Adaptive Governance and Continuous Compliance
- Identity-Powered Security
- Scalability

Adaptive Governance and Continuous Compliance

Most governance systems provide periodic review and certification of access rights, which results in a compliance and security blind spot between certifications. NetIQ Identity Governance by OpenText™ can reduce or eliminate blind spots by being able to react to events detected in our identity management and SIEM solutions. This provides "continuous compliance" capabilities. For example, when a user's responsibilities change, an identity lifecycle event is detected and can initiate an access review process for that user in NetIQ Identity Governance. Our solution can then trigger access change requests that can be fulfilled automatically or via a help desk solution and ultimately be verified by the governance system to ensure that only users that need access maintain access.

Identity-Powered Security

NetIQ identity governance and administration is not the only area where OpenText™ provides solutions. We help organizations address risk and complexity, from both privileged and regular users, with an integrated set of solutions that manage the identity and access lifecycle, authentication, identity governance, and security monitoring. We call this approach Identity-Powered Security.

Scalability

We have over 5,300 identity customers and combined, we're managing more than 436 million users. Over 33% of our customers are larger than 10,000 users, with the largest account managing 55 million active identities. All that to say, *our solution can scale*.

When determining your approach and what solution you are going to leverage to achieve governance, we recommend that you ensure your chosen solution has five key features:

- Connectors with Bi-Lateral Communication
- Identity Analytics
- Intelligent Reporting
- Intuitive End-User Interface
- Automated Workflows

Key Functionality Required to Achieve Governance

When determining your approach and what solution you are going to leverage to achieve governance, we recommend that you ensure your chosen solution has five key features.

Connectors with Bi-Lateral Communication

Some vendors will promote the fact that they have connectors for a very large number of applications, or that they do not charge for additional connectors. Usually the reason they do this is because their connectors are unidirectional. Our connectors provide bi-lateral communication to keep everything in sync real-time. They are configurable and do not require code to modify them, making them easier to upgrade and maintain.

Identity Analytics

Your governance solution will work much better for your organization if it includes an analytics component. We're not just referring to the initial insight and discovery phase where you map out who has what, but functionality that is ongoing and provides your decision makers with real-time decision support. If the solution is able to highlight information such as how many other users in the requestor's role have the same access, what the risk level is, and whether there are any flags, then the line of business manager is able to make a better decision about whether to grant the access request.

OpenText™ provides additional analysis for managers when reviewing requests. This image shows that the access seems unusual and goes on to explain that the requestor would be the only one in his role with this type of access.

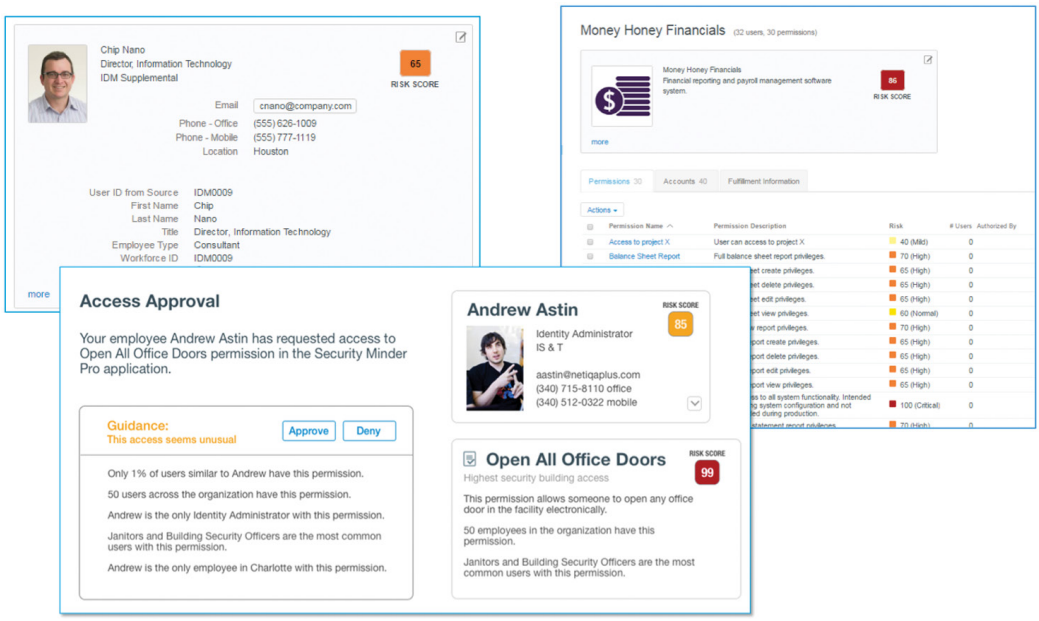

Figure 2.

Intelligent Reporting

that you will definitely want to add to these and create some of your own reports. We offer an open reporting schema, allowing you to produce your own reports, or we can produce them for you if you prefer. With the market alternatives, you have to wait for a patch in order to get access to the latest reports. At OpenText, we make them available instantly through the reporting server. Simply click the download button and add new or updated reports to your repository on demand.

With the market alternatives, you have to wait for a patch in order to get access to the latest reports. At OpenText, we make them available instantly through the reporting server. Simply click the download button and add new or updated reports to your repository on demand.

Intuitive End-User Interface

A key function of identity governance is to involve the line of business in decisions about whether a user should be granted access. So when examining the user interface, you should look at not only how easy it is for the end user to find what they are looking for and submit their request, but also look at what the approver sees when responding to the request. Special attention should be paid to the recertification functionality so that it is easy for the managers to use, but also ties into the analytics functionality to provide the information they require to perform the task at hand.

Automated Workflows

The ability for an identity solution to automate a provisioning workflow during a request is certainly not new. If a request for access is approved, then automate the response action to grant the access. However, having this functionality tie into the governance component is what we're referring to here; it will reduce risk and enable your organization to have better and faster control. For example, if the governance component identifies an issue and initiates an attestation process, and if you have an automated workflow engine that can immediately address the response to remove someone's access, the risk is immediately mitigated. However, if the workflow engine is not integrated with the governance component, then you will need to rely on human interaction to read the notification and then manually take action.

NetIQ Identity Governance is often implemented as the result of something bad happening. Regardless of the situation you find yourself in, we can help you navigate to a state of control and diminished risk.

Conclusion

NetIQ Identity Governance is often implemented as the result of something bad happening. You failed an audit, you had a breach, or you discovered some sort of risk and are now taking action. Addressing this, especially in any of the previous high stress situations, can be complex, but it doesn't have to be. Regardless of the situation you find yourself in, we can help you navigate to a state of control and diminished risk. Our extensive experience and customer base in this area shows that we truly understand the struggles our customer face. We also understood the importance of integrating governance with administration well before now and had been working behind the scenes to ensure our customers were ready.

We welcome the opportunity to help your organization to efficiently provide appropriate access permissions so that your users can do their job. Our smart, yet simple access governance enforces the least privilege principle, which helps to reduce segregation of duty violations from users with "access creep," a common problem when employees accrue access for special projects or when changing roles. Compliance is often the byproduct of an identity governance program and we can enable you to minimize user permissions to only what is appropriate—a proven method to help reduce compliance violation fines and thwart potential insider attacks. This is particularly true for privileged users, because these users typically have the broadest access rights to your organization's most sensitive data, systems and assets.

We welcome the opportunity to help your organization to efficiently provide appropriate access permissions so that your users can do their job.

About NetIQ by OpenText

OpenText™ provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ by OpenText homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of Cybersecurity, an OpenText™ line of business.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/identity-governance

Connect with Us
www.CyberRes.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

762-000042-002 | O | 05/23 | © 2023 Open Text