opentext™ | Cybersecurity

Position Paper

# IGA Buyers Guide

## Selecting the Right Identity Governance and Administration Solution

# Raising Your Identity Governance Game

Beginning as a necessity to simply provision new employees into various foundational systems, IT is finding it increasingly difficult to manage entitlements for a growing list of services needed by employees and contractors to do their job.

Adding to this are escalating risks from an increasingly connected world and maturing privacy regulations. Not only has virtually all information become digital, but it is also usually cloud-based. Altogether, this digital transformation has created an identity and access sea change: the perfect storm of connected systems holding sensitive digital data in a world of rising breach costs and regulations. It is in this context that organizations have placed a new emphasis on automating permissions management and transitioning control of it to the information and business owners.

Evolving identity governance to the next level requires that you empower your business owners to participate in mapping their business processes to governance policies.

## Digital Transformation Security Complexities

NetIQ Identity Governance and Administration by OpenText™ is the merging of identity life cycle management and access governance. And while automation remains a foundational approach to identity management, there is also a need to be more effective in permissions governance and attesting to its execution. So, while the categories in the list below aren't new, the level of complexity is:

- **The number of services:** The number of services requiring coordinated permissions management continues to multiply. Despite the promise of federation technologies, even newly developed services typically implement their own copy of an identity store for authentication and authorization. This design matters because digital transformation continues to proliferate the number of digital services and resources needed for each employee to do their job.
- **Location of services:** The move away from intranets as the predominant host of services has reached a mainstream level. This means that most organizations have a hybrid digital infrastructure consisting of a mix of cloud and proprietary services. It is this diminished role of firewalls that makes timely permission updates critical—and the failure to do so, perilous. So much so that manual administration of them is increasingly unviable, both in terms of invoking permission updates in a timely matter and the growing consequence of human error.
- **Compliance:** Organizations continue their struggle to enable a more efficient workforce and develop more engaging services for their consumers, while staying compliant with the regulated information that they hold. Digital transformation has made gathering and assembling the information required to attest compliance a progressively unwieldy exercise. The sheer size and complexity of distributed services and resources have pushed audit preparations beyond a spreadsheet exercise. Beyond the complexity of an audit, breach of regulated data often results in rigorous vetting to ensure that compliance is continual.
- **Risk and least privilege:** Managing business exposure extends beyond the risk of failing an audit; it includes the fallout of an actual breach. Beyond the consequences imposed by a regulatory agency, the financial hit from lost consumer trust can be sizable, or even fatal, to executive management. One of the best tools for protecting sensitive information is to be disciplined in applying least-privilege security principles—meaning, only those who need access to sensitive information have it. And, if or when that need goes away (for example, a role change), access goes away with it. And while least privilege is one of the most effective ways to limit the damage of a breach, it is next to impossible for most organizations to practice it without automation.

To meet these challenges, organizations are bringing in business-related insights to deliver effective entitlement decisions, automate their enforcement, and attest to its execution.

Section 3.1 of NIST Special Publication 800-171 offers guideline of defining your access control criteria.

## Responding to the Latest Access Trends

While digital transformation has enabled remote workers to be more productive, the COVID-19 pandemic pushed IT teams to expand their remote strategy and speed up their implementations. Not just internally, but also consumer-facing services and interactions. Allowing the access of so much sensitive information to remote users on BYODs in such divergent circumstances requires a new paradigm of security principles and approaches, including entitlement management.

# Measuring Your Access Governance Capabilities

Accurate risk assessment is dependent on a comprehensive digital asset catalog.

As you evaluate the maturity of your access governance infrastructure, take a moment to assess the levels of risk that your sensitive resources pose to your organization. It's quite possible that your IT or Security teams have risk assessment artifacts that list the vulnerabilities (predisposition and severity), as well as the potential range of impact from improper access (malicious or otherwise) to those resources. The more concrete your understanding of the threat landscape that your digital resources pose to you, the more accurate your ratings to the questions below will be.

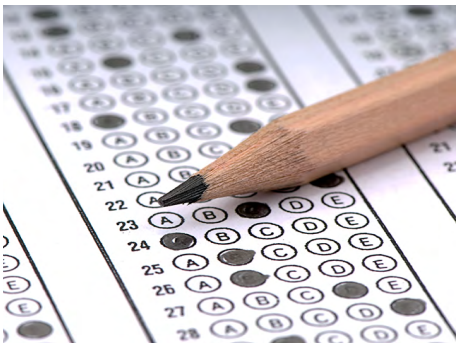
### Assessing Your Environment

| Strongly Agree | | Strongly Disagree |
|---|---|---|
| Our security team takes an aggressive least-privilege approach to granting access to controlled information and privileged accounts. That is, we ensure that no higher entitlements or permissions are granted beyond what is necessary for individuals to accomplish their functions. | | |
| We have applied least-privilege principles to the development, implementation, and operation of our organizational systems. In concert with our organizational design, our processes, roles, and accounts are purpose built to achieve least privilege. | | |
| We take a holistic approach to separation of duties that spans across the full range of systems and application domains to protect against malevolent collusion. | | |
| Our separation of duties controls are automated to ensure timely enforcement of access permissions. | | |
| We can easily define and enforce policy for who should have access to what and when approval is necessary and have involved our line of business managers. | | |
| It is simple for users to request access and for managers to approve access requests. | | |
| I am confident that our business managers and application owners have the information they need to make an informed decision on who should be granted access to controlled resources. | | |
| I am confident that our business managers and application owners do a thorough and complete job when performing the required scheduled access certification reviews. | | |
| Getting the right people the right access is an efficient process that doesn't consume too much staff time. | | |
| For our controlled information and resources (regulated or sensitive), we know who has access to what. | | |
| Our digital fulfillment systems are "closed loop," meaning we can attest that we fulfilled and revoked access permissions that enforce government and corporate policy. | | |
| Through our application and access management systems, we maintain comprehensive and accurate historical records of when individuals accessed sensitive resources. | | |
| All of our governance records and logs are tightly secured and monitored to prevent modification or deletion. | | |
| | Total: | |

### Assessing the Results

Now that you've done your best to measure your access governance capabilities, review the breakdowns below to see where your organization fits. Of course, these generalized descriptions don't take into account the industry that your organization is in; nor is it a direct indicator of whether you will be subject to a fine.

| | |
|---|---|
| < 26 | You likely have a solid Identity Governance and Administration solution in place. Consider a review of your tools and processes to ensure that your implementation is future proof. |
| 27–38 | You have done a good job at putting some key identity and access controls in place, but there is still some work to do to reduce organizational inefficiencies and reduce your risk of access misuse. |
| 39–51 | You might have a few identities and access management solutions in place, but demonstrating access control and ensuring that users get access when they need it is difficult if the solutions aren't integrated. |
| 52 < | Your organization is likely at risk from outside attack or misuse of access by employees, with a high potential for audit findings. Consider an Identity Governance and Administration solution from a trusted vendor. |



# Addressing Your Governance Gaps

In addition to measuring your overall identity governance score against the table above, you can also focus on areas of weakness, as identified by the rows with your lower scores. This section further explains the extent of these capabilities.

Before you can empower your business owners to make the right entitlement decisions, you must present them relevant information in a way that they can quickly digest it.

**Developing Least Privilege Principles and Policies**

Beyond the technology itself, the strength of an organization's least privilege implementation depends on its approach to defining it. Least privilege should be designed and configured based on how the business owners view their risk and the posture they want to take to protect against it. These questions are important because they form the basis for management taking action and investing in a solution to implement their business and security goals. Measuring risk can be divided into two broad categories:

- What vulnerabilities does your sensitive information pose to you and how do they match current breach trends?
- When a breach happens, what are the predicted costs to your organization for each of the data profiles you are protecting?

From this foundation of measured risk, an organization should define its philosophy and corresponding least-privilege processes, outlining how aggressively they want to apply it. To do this means it must first be measured. Step 1 is for the responsible business owners to determine the risk that each of the different types of resources poses to them and the restrictions or conditions that must be met before granting access. Examples of account types or roles include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Conditions of access beyond just permissions are things such as time of day, day of the week, point of origin, or device familiarity.

**Effectively Applying Your Least Privilege Processes**

In order for your access governance solution to be effective, it needs the flexibility to protect all of your sensitive resources. Typically, this goes beyond data accessed through services and your unstructured data (Doc, XLS, HTML, CSV, JPG, etc.). Proper coverage is more than casting a wide net; it also requires granularity to enforce the specific policy in place. So, in addition to importing identity information, you need the flexibility to manipulate permissions and possibly set the context (device, place, time, etc.) that controls when those permissions can be executed.

Beyond robust automation, your organization needs to monitor your protected information from these perspectives:

- Employing a dedicated monitoring solution to watch for when specific resources are accessed and by whom.
- Monitoring context and behavior to potentially respond if a risk threshold is exceeded.
- Ensuring that all monitoring capabilities clearly and reliably associate a session with an identity.

**Workflows That Work**

To assess your permission workflows, you need to evaluate the user experience and the reach of governance across your organization's resources. You know that you have a well-implemented permissions workflow solution when it is easy for your users to request and gain access to the resources they need. At the same time, resource owners are still able to protect them. The main vulnerability in this scenario is the proliferation of granted permissions—that is, extending them beyond their desired level. In short, you are maintaining an environment where only the right people have access to the right resources, while keeping the organization both efficient and secure.

Here are some key areas to focus on:

- **Encompassing governance:** The more complete your governance implementation, the less often users will have to go outside of it to gain access. Ideally, all resources that require special permission to gain access should be managed through your governance solution. Conversely, when users are forced to go outside of an automated request system, it is more hassle for them and less secure for the organization.
- **Simplicity for the requester:** The workflow tool needs to be easy to find, simple to use, and accessible when and where the requester needs it—which usually means anytime on any device. Once they are in the tool, the list of resources needs to be easy to find and granular enough that requests are limited to only what is required.
- **Effective approver:** Core to this requirement is bringing together all of the information needed for a business-level approver to make the best permissions decision and do it quickly. The critical element is to present the relevant information in such a way that a business owner can promptly understand what access is needed and the level of risk it imposes. A key objective is to protect against approval rubber stamping and to make a judgment based on:
  - Does the requestor merit the access?
  - What is the total risk involved by granting access?

Not only are workflows essential to automating permissions management, but they also offer an opportunity for you to present the right set of information to the asset owner at the exact time he needs to make an entitlement decision.

### Managing Separation of Duties across Your Organization

Because most organizations run lean, it's not uncommon for employees or contractors to wear many hats, covering a diverse set of responsibilities. In these environments ensuring separation of duties (SoD) for security, and often compliance, can be elusive. NIST summarizes security intent as "separate the duties of individuals to reduce the risk of malevolent activity." For digital services, common collusion risks are responsibilities such as configuration management, quality assurance, testing, system management, programming, network security, etc. Other standard SoD implementations are used to enforce policies designed to mitigate against the risk of fraud and made possible through collusion.

Because SoD violations can span systems and application domains, effective implementation needs to measure the entirety of organizational systems and system components. So, when approvers are "in the trenches," they need the right information to ask the right questions and identify a change that hasn't been properly vetted. And beyond implementing SoD as a security best practice, organizations that interact with financial services have Sarbanes Oxley Act (SOX) compliance requirements that make it even more crucial to get it right. The three most common SoD scenarios that organizations need a robust solution for include:

- **Requester/approver workflows:** While rubber-stamping permissions approval is a general security issue, providing SoD-related information in an easily digestible format for quick decisions is paramount.
- **SoD Reviews:** Organizations should have regular SoD reviews to protect themselves from various threats from over-privileged users. With the right tool, this review can be a quick process.
- **SOX Audits:** Too often, generating reports attesting to compliance is an arduous process, the worst-case scenario being that you have a find. With the proper foundation in place, audits can be essentially a reporting process.

Not only are workflows essential to automating permissions management, but they also offer an opportunity for you to present the right set of information to the asset owner at the exact time he needs to make an entitlement decision.

### Maintaining Permissions Integrity

Having the most tuned environment (least privilege without reducing efficiency) requires active and competent participation by the information owners themselves, including periodic access reviews. For the best chance of ferreting out excessive rights, information owners need access to a simple and informational tool. We need to acknowledge that permissions management isn't high on the information owner's priority list, so the faster and less painful access reviews are, the more likely they will be a worthwhile security practice. The broadest set of governance data (such as applications and services, employees or their status, risk threshold, etc.) needs to be searchable. In addition to making it easier to stay on top

of permissions management, providing training on the risks of excessive rights for both information compromises and audit finds is equally valuable.

Placing the white light on your most significant risks: The best use of data owners' time is to draw their attention first to the accounts or permission sets that create the highest risk scenario. Bringing that information to the forefront and presenting it in a way that is easy to understand allows the highest risk configurations to receive the most attention.

Separation of duties is more than a regulatory compliance requirement, it's a core tool for you to prevent fraud and other behaviors that could harm your organization.

**Quick drilldowns:** Before you can offer drilldowns to information owners, you need a comprehensive entitlement repository from which everyone's access to everything is searchable and manageable. Common types of operations that should be offered include:

- An entitlements catalog from which security teams and owners can search for and manage collections, groups, permissions, and other attributes.
- Business roles search and view capability—manage birthright permissions gained from the role, as well as searchable roles to find the entitlement sources.

Management consoles should be customizable to allow for specialized views and management of accounts and permissions.

### Compliance and Attestation

The following organizational objectives typically drive governance attestation exercises:

- Self-audit conducted either within a department or across the entire organization. These audits are used to measure the effectiveness of current security policies and processes.
- Internal attestation exercises conducted as part of a risk management initiative to assure a partner or customer that your organization meets specific security criteria or levels.
- External audits conducted by a regulatory agency, such as those found in the financial or health industries, to verify compliance with government mandates such as PCI, HIPAA, SOX, GDPR. Because audit finds at this level might result in a fine, these external audits tend to drive the internal ones.

Micro-certifications are used to strengthen your confidence in the attestation. The micro-certifications approach is to continually monitor for any permission changes for the protected resources and verify on the fly that those changes comply with defining criteria. For confidence in the added security of micro-certifications, you need an implementation that monitors for out-of-band modifications made outside of the governance platform. Administrators are alerted to investigate the permissions change whenever a change is identified.

Ideally, reporting is simply a snapshot of permissions status controlled from a central point of the administration dashboard. Different industries each have their specific set of report requirements; the best option is a solution that offers a variety of pre-built reports that can be customized.

# Choosing the Right Information Governance and Access Solution

OpenText's full platform approach offers some notable advantages to organizations as they strive to reach their identity and access objectives. Far lighter than the big enterprise solutions, OpenText™ has always enabled IT teams to be more nimble in their approach to identity management. At the same time, OpenText offers a more encompassing portfolio than the point vendors, with products that work well together. For example, you can feed NetIQ's Identity Governance by OpenText™ risk information into the NetIQ Risk Service by OpenText™ to include the inherent risk of both resources and users as data is being accessed. This integration offers far greater risk assessment fidelity than any other solution in the market, as well as the ability to automate a response to protect the organization being threatened.

Micro certifications gives you an added level of confidence in your attestation submissions.

**Identity and Insight**

The same can be said for using NetIQ products by OpenText to achieve your organization's NIST identity governance goals. For example, NetIQ Identity Governance is greatly enhanced by NetIQ Identity Manager's event-based connectors that interact with the identity stores in a publish/subscribe model. This model allows NetIQ Identity Manager to enforce governance policies more forcefully than is possible in competitive solutions. Even for identity stores not integrated directly through NetIQ Identity Manager, access information from NetIQ Access Manager by OpenText™ can be used to kick off an automated micro-certification to verify that the correct level of permissions is in force.


**Developing the Best Least Privilege Model**

As with any organization-wide implementation, successful development of a valid and comprehensive foundation of permission policies is heavily dependent on commitment from management at the top. It takes their sponsorship and prioritization to get the required information and business owners to participate and focus on evaluating the services they provide, in order to organize and define access criteria.

Your team's first step is to use the NetIQ Identity Governance definition template to create application entities that will enable you to collect application and resource information. Then you can arrange the consumers into logical entities in the form of roles. After this phase, your stakeholders can use this information to define business roles and then then rules that control permissions for each resource.

### RAISING THE EFFECTIVENESS OF YOUR ROLES

Well-defined roles have the potential to simplify risk and compliance assessment for the governed environment because they define what the standard allocation of permissions is. NetIQ Identity Governance simplifies what can quickly become an overwhelming task by filtering down to only your relevant information for identifying people within the same business function. This information can be used to determine the baseline of what users should have access to and whether they can request that access without additional approval. NetIQ Identity Governance does this by consolidating relevant information through role-mining tools that enable you to define a more capable model. With this model you can see across your entire organization and identify where people have relevant similarities:

- After you have collected the information into NetIQ Identity Governance, you can do searches of what you have: similar attributes, similar location, similar department.
- Within NetIQ Identity Governance, you can adjust the different parameters that are assessed and use that information to refine your policies.

### FINISHING TOUCHES ON GATHERING ENTITLEMENT INFORMATION

With that groundwork in place, you can complete your picture of who needs access to what and measure the associated risk. The result of all this work is being able to conduct successful certifications. NetIQ Identity Governance helps you assemble a least privilege foundation by:

- Automating the collection and validation of account information (identity, group, application, and permissions) across your environment.
- Collecting and updating policies that control access to these resources.
- Calculating risk.

As your roles are tuned over time, your baseline could reach a point where accounts within those roles are granted permissions without having to make any type of requests, reducing the burden on your supervisors and approvers. In addition to this reduced overhead, a fine-tuned baseline will keep costs and risks down for your governed services.

**Automating Requests, Approvals, Reviews**

With entitlement management foundation in place, NetIQ Identity Governance provides automated request and approval workflows:

- Requesters are offered a familiar user experience similar to online shopping, where they add desired services to a shopping cart and send off the request for access.
- Along with the request, approvers can be presented with a business case that includes the cost and potential risk criteria to help them make an educated decision.
- If needed, requests can then be passed on to the next level.

Beyond NetIQ Identity Governance's robust automation, it enables you to monitor protected information from these perspectives:

- See who accesses specific resources and when.
- Monitor context and behavior to potentially respond if a risk threshold is exceeded.
- Ensure that all monitoring capabilities clearly and reliably associate a session with an identity.

You have now reached a point where you can account for users who are granted access outside of that structure. These one-offs often need to be brought to the attention of the information stakeholders (owner and security team) and incorporated into NetIQ Identity Governance. With relevant information about the account and resources at their fingertips, approvers and reviewers have what they need to make the right decision.

**Micro-Certifications**

Once all relevant information has been onboarded into your governance environment and permission flows are automated, you still need the ability to react to out-of-bounds risks. These are situations that fall outside of the criteria accepted by the organization. This assessment check happens through permission checks called micro-certifications. One type of check is on a specific person, measuring permissions across the entire digital landscape. It's not uncommon for a periodic process to be kicked off for each account, highlighting permissions to resources that have never been accessed or that haven't been accessed for a defined period. Increasingly, these processes are being used to drive down the costs of specified account-based licenses.

The other type of micro-certification targets a specific resource, one that is sensitive and deserves close inspection. This type of micro-certification is often initiated in these ways:

- As a routine designed as a layer of protection for highly sensitive data.
- When a permissions trigger is kicked off, indicating that excessive permissions have been allocated for a digital resource.
- In response to an alert or a report of unexpected actual access to the access management architecture.

Micro-certifications are a specialized process intended to limit an audit to specific criteria. OpenText enables you to automate this process to a focus area that kicked off the event. This ability to receive an event notice and quickly react with a specialized audit can be a powerful tool for increasing security and keeping costs down. For NetIQ Identity Governance, this process inherits reviewer assignments and settings from the specified review definition. You can run a micro-certification for any review type. If it is part of your standard security practices, OpenText enables you to run multiple certifications in parallel, either on-demand or with a preset schedule.

By incorporating NetIQ by OpenText™'s micro-certification into your security processes, you establish greater protections against the consequences of a breach, as well as an audit find from a regulator agency. In contrast, manual certification processes are time-consuming and labor-intensive, making them impractical. Without automation, your security teams will be subject to certification fatigue. Instead, automation enables you to maintain your security edge.

## About NetIQ by OpenText

NetIQ 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, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ by OpenText page 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.

**Connect with Us**

www.opentext.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.