Managing Change and Complexity with Identity and Access Governance

_The only thing that is constant is change_. This old adage has never been truer than it is today. Businesses must manage their systems within ever growing and changing complexities. The Identity and Access Governance (IAG) environment is front and center in the ongoing battle to deal with constant change effectively.

How is change and complexity causing you to rethink your approach to identity, security and governance? Do you have the necessary tools to meet those challenges? Do you have the processes in place to take your organization forward into the rapidly evolving world that lies ahead?

There are several areas to consider when planning for the future. IAG solutions may seem like a burden brought on by increasing regulation and compliance issues, but when used effectively, IAG solutions become the catalyst to meet the challenges of a complex and changing world. Regulatory compliance has become an important corporate initiative as the complexity and scope of the regulatory environment continues to increase. Additionally, with the rise of cyber-attacks and insider threats, organizations are now searching for a more effective, sustainable, and scalable approach that will achieve their compliance objectives while improving the overall security posture of the organization.

In this white paper, we will examine some of the challenges that modern organizations face in their efforts to develop and adapt a compliance program that can solve today’s needs and support new requirements in the future.
Table of Contents

Introduction .............................................................................................................................................................. 1
Making a Change .................................................................................................................................................... 1
Definitions................................................................................................................................................................ 1
  Identity Management ........................................................................................................................................... 1
  Access Governance ........................................................................................................................................... 2
  Identity and Access Governance (IAG) ............................................................................................................... 2
  Identity and Security Goals.................................................................................................................................. 2
External Drivers of Change and Complexity........................................................................................................... 2
  Attacks and Security Breaches ............................................................................................................................ 2
  How Does Identity and Access Governance Help? ............................................................................................. 3
  Cloud Computing ................................................................................................................................................. 3
  How Does Identity and Access Governance Help? ............................................................................................. 3
  Going Mobile ....................................................................................................................................................... 4
  How Does Identity and Access Governance Help? ............................................................................................. 4
  Budget Constraints .............................................................................................................................................. 4
  How Does Identity and Access Governance Help? ............................................................................................. 4
Change, Complexity and IAG.................................................................................................................................. 4
About NetIQ............................................................................................................................................................. 5
Introduction

Identity and Access Governance (IAG) has become a vital part of all organizations, due to government and industry oversight, as well as internal controls. The drivers that move IAG needs are nearly always external to the company. IT and business managers must respond to the pressures of change and complexity in today’s business environment, security concerns, advancing technologies, and increased regulation and compliance issues. But as needs and pressures increase, budgets are on the decline. Managing change and complexity through governance can be a great opportunity if done correctly. The key is having not only the correct tools, but the processes in place to meet these ever growing needs.

Making a Change

To manage change, it is imperative to first understand it. Change is not a one-time event, but an ongoing process. When a need for change arises, human tendency is to resist it as long as possible. Change finally happens when it becomes painfully clear that it can no longer be avoided, and forces are mustered for one great push. Change finally happens, and the company population settles back into a comfortable routine. But change is constant, and the need will soon arise again. The inertia necessary to move an organization forward into new environments is difficult and costly, and every time a new change is needed, the pain begins again. By the time a change is complete, the need for a new change will already have surfaced, in order for the company to keep up with the speed of business. To effectively deal with the complexities and changes that are constantly on the horizon, businesses must realize that they do not simply change a process, change IS the process. Change must be planned for, sought after, embraced, and integrated into the daily fabric of the corporate culture.

Beyond the mindset that is needed to manage change and complexity, effective tools are vital to the success of a company that is meeting and exceeding the requirements of today’s business environment. Systems must enable both IT and business managers to easily visualize complex systems, monitor areas of concern or risk, and trigger appropriate actions if policies, procedures or requirements are nearing the bounds which have been set in critical business areas.

As you look at your business, how are change and complexity causing you to re-think your identity, security and governance? This document will look some of the key areas of concern and how IAG can provide effective solutions.

Definitions

Before delving into the issues that often drive change and complexity, some definitions are in order:

Identity Management

Identity management concerns lie within the IT realm. These deal with provisioning hardware and software as well as managing the identity of those using company resources, and the identity of the resources and devices themselves.

A person’s identity may include the following attributes:

- Who are you? – name, location, contact info, etc.
- Roles – title, manager, etc.
- Relationships – employee, contractor, vendor, etc.

Once an identity is established, the next step is to determine the appropriate scope of each individual’s access by creating relationships with resources. This includes: applications, systems, data, groups, physical facilities and other company resources.
Access Governance

Clearly understanding access is the key to Governance. It is ultimately the responsibility of business management, rather than IT management. The tools in this area are designed to meet business needs with straightforward, user-friendly interfaces, for those who may be less technically inclined. Concerns in this area include:

Who has the access?
- What level and type of access?
- Who provided the access?
- Was it reviewed, and is the access appropriate for each identity?

Is the access secure?
- Can I monitor what is being done with the access?
- What is the risk of giving access?

Flexible fulfillment of the access?
- Can I provision access across physical and cloud environments?
- Can I assign privileged and delegated access?

How do I gain access?
- Can I enable sign-on from any device, from anywhere, for everyone?
- Can the access be federated?

Identity and Access Governance (IAG)

IAG is the convergence of both identity management and access governance. Effective IAG solutions should seamlessly integrate both disciplines to meet overall company objectives.

Identity and Security Goals

There are common goals among corporations with regards to their IAG solutions. These include:

1. Controlling the risks and challenges of computing across multiple environments. This includes divergent operating systems, hardware, the cloud and mobile devices.
2. Users must have appropriate and timely access to the computing services needed to do their jobs.
3. Computing must be secure and compliant with all relevant policies, procedures, and regulations, even when using mobile devices.

External Drivers of Change and Complexity

Attacks and Security Breaches

Attacks are increasing, both internally and externally. Security breaches are of paramount concern in today’s business community. The goal of all marketing departments is positive press, but when it comes to security breaches, it may be even more critical to the success and even the very existence of a company to stay out of the press. Nothing erodes the trust of customers and regulators more than a breach of sensitive information---be it a leak, or theft of customer’s intellectual property.

Verizon reports that 58 percent of all breaches are by organized crime or activist groups, often referred to as “hactivists.” Sadly, most cyber-attacks are preventable. In many cases, the affected company had the available information, and could have prevented the attack if they were paying proper attention, had preventive procedures in place and had actually followed them. Merely having a firewall is not nearly enough security to stop attacks. A recent study on corporate security determined that “an enterprise can often learn more about its network security not from traffic that was denied, but from what was allowed in.” Attacks from internal employees are also on the rise.
Rising risks of security breaches and falsified or fraudulent data infiltrating company systems has resulted in many laws and regulations becoming a reality in business. Some of these include:

- PCI DSS
- Sarbanes-Oxley
- NERC-CIP
- FISMA
- GLBA
- HIPAA
- BASEL III
- J-SOX
- Solvency II

**How does Identity and Access Governance help?**

A strong IAG system such as NetIQ® Access Governance Suite 6, combined with Identity Manager, provide systems and controls so that business managers are aware of all access, and whether that access is appropriate. On a single dashboard, each user’s profile, or “identity cube,” may be accessed to ensure that each person is defined with the proper roles and access. So-called “Entitlement creep,” or access given in the past that carries forward to new assignments, even though some of it is no longer warranted, can be avoided by regular certification. This ensures that individuals are given only the access needed to get their current jobs done.

Another concern regards orphan accounts that need to be eliminated. As employees, contractors and vendors leave their association with a company, systems should be put in place that automatically remove all access to company resources. These and many more features of a strong IAG solution ensure that access is limited to only those who actually need it.

Monitoring every single piece of data can be a daunting task. Effective potential risk scoring, risk management and mitigation may all be handled via IAG. Systems are in place to notify business managers regarding areas of concern, and to enable managers to effectively track those things that matter the most.

**Cloud Computing**

New issues emerge in the cloud. While the cloud can mean many things, the National Institute of Standards and Technology (NIST) defines it as “the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet)”.

As software applications are delivered in a SaaS (Software as a Service) model, keeping company data secure is an increasing problem. How is data secured in the cloud? How do companies ensure that sensitive materials are not being accessed by those without proper authentication or authorization?

An effective IAG solution monitors access to all company resources, including those in the cloud. Cloud resources may be off-site, but they are not out of mind. The cloud gives a corporation incredible scalability, as additional resources may be accessed when needed, but that access means that customers also pay additional fees. Not only does an IAG solution monitor the appropriate access and usage of cloud-based resources, it also ensures that you are using only as much as you need, keeping usage fees to a minimum, and helping you maintain proper control.

---

1 “Verizon data breach report 2011: Attackers refining their targets.” Searchsecurity.techtarget.com
Robert Westervelt, News Director Published: 19 Apr 2011.


Going Mobile
Access from anywhere, using anything. With the advent of laptops, smart phones and tablets, users are no longer content to access company resources from the confines of their offices or cubicles. They want to access data on-the-go. Providing access in a secure fashion can be a challenge, especially if data is requested to be taken offline. Should a company allow that? Is the company still in compliance if it does? What if a team decides to go around the system, trying to get what it needs in a non-compliant way?

How does Identity and Access Governance help?
IAG can define parameters for access based on many things. Beyond role or title, access may be determined by device as well. It may be possible for users to access less sensitive data by broader means, while highly volatile material may need to be controlled to ensure compliance. Where users need mobile access, it may be granted, and password security may be controlled at the IAG level utilizing groundbreaking technology, ensuring that even if unauthorized people see a password being typed in, they will not be able to gain access using their own devices at a later time. There are many challenges in the mobile computing world, and IAG technologies can provide a safe, secure solution.

Budget constraints
As budgets tighten, demands increase. In today’s business climate, budgets are shrinking, while the needs and demands of identity management and security are on the rise. As average computer users become more technology literate, their needs increase, while the speed of delivery and access also becomes a growing concern. For example, hiring managers are no longer willing to send off a help desk ticket and wait for access to be given for a new employee. Meanwhile, as projects end and new ones begin, team members’ access must be quickly altered. Identity and security must be managed at the speed of business, even as the burden on IT staff members increases to keep systems current and upgrades in place.

How does Identity and Access Governance help?
IAG systems are vital for effectively provisioning, and managing access to company resources. Many processes are routine and repetitive, and with effective automation, companies can eliminate regular, time-consuming involvement of IT. For example, the process to set up a new hire can be determined by the role of the new employee. Once systems are in place, HR personnel can initiate new employee profiles with appropriate access, based on the jobs they will be performing. As an employee leaves, HR may also invoke the automated access process to ensure orphan accounts are eliminated. There is no need for IT, or even the business manager to get involved in such a repetitive function. Simple processes such as password authentication and changing a password can also be easily managed by an IAG solution.

In addition, as complexities grow, an AIG system allows security risks to be identified and mitigated. Taking a proactive rather than a reactive approach to risk management allows companies to focus their security efforts on areas and personnel that are a higher security risk. As budgets tighten, it is often necessary to pay more attention to critical areas, while system protocols are in place to ensure that compliance is met in a cost effective manner.

Change, Complexity and IAG
The ability to manage change and complexity is becoming more important by the day. An effective Identity and Access Governance solution is an integral part of making that goal a reality. IAG provides automated, easy-to-use systems that support business objectives in a secure environment. Identity and Access Governance does much more than get and keep companies in compliance. In a complex and changing business climate, it is the key to protecting a company’s most valuable assets, including intellectual property, sensitive data and most importantly, the trust of their customers.
About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit www.netiq.com.