Why It Pays to Take a Business-Centric Approach to Compliance

Today's IT departments must defend against complex internal and external threats while mitigating regulatory and compliance concerns. Many businesses are simply overwhelmed. Clearly, organizational risk management has reached a critical juncture.

A July 2012 IDG Research Services poll of CIOs and IT managers underscores the gravity of the situation. The results provide important data about how enterprises view compliance overall, and identity management and access governance in particular.

Survey respondents list improving overall organizational risk posture as their number-one near-term compliance objective. Other top objectives include improving audit performance and freeing up IT to focus on higher-value activities.

It's not surprising respondents want to free up IT, given that nearly three-quarters of them (76%) describe their current compliance and attestation processes as either completely or mostly manual. Nor is it surprising respondents say the manual/slow nature of their current compliance and attestation approach is their biggest challenge.

"Companies are finding that home-brew tools or manual processes just don't scale—they take way too long," says Bryan Cardoza, senior product manager at NetIQ. "If it takes you six months to complete certification, and your reporting period takes six months, you're never finished. So how could you possibly consider expanding that? Whenever you have a manual process, you inherently introduce a higher error rate into the process."

The fact of the matter is that time-consuming manual processes don't cut it in today's volatile business environment. It's why more and more organizations are taking a closer look at identity and access governance (IAG) solutions. IAG is a business-centric approach to identity management that addresses rapidly evolving technical, legal, and regulatory requirements.

IAG provides automated, easy-to-use systems that support business objectives in a secure environment. It's an approach that gets IT out of the business of making business decisions, and improves the quality of information and decision-making for all stakeholders.

Small wonder, then, that nearly two-thirds of the IDG survey respondents rank the ability to deliver user-friendly, self-service compliance and attestation tools as very important or critical. Respondents are also very likely to perceive a close link between identity management and access governance.

What a Suite-Based Solution Can Offer

When it comes to access governance, mitigating risk is paramount for all organizations—regardless of industry. Access policies should be well-defined, centrally controlled, and consistently enforced. But already-overburdened IT teams can't keep pace with an ever-increasing flow of security risks. Add such technological advances as cloud computing and mobility, and the number of vulnerable surface vectors subject to security attacks can escalate dramatically.

Taking a suite-based framework approach to IAG can alleviate all the above challenges. The framework supports critical risk management processes, including:

- Establishing compliance initiatives and meeting regulation requirements
- Controlling user access/instituting lifecycle management
- Ensuring accountability
- Automating processes to manage access risk

To improve enterprise-wide visibility into user access and gauge policy compliance, suite-based solutions offer unparalleled management controls. Gaining a clear picture of internal threats, identifying individual user access, and determining whether that access is appropriate are all key concerns of IT administrators.

A suite-based access governance approach enables an administrator to gain a clear organizational “snapshot” of user access and take corrective action as necessary. It also ensures that all governance actions are “sticky,” i.e., unable to be reversed unless approved by a recognized authority.

Nearly half the IDG poll respondents (45%) stress the importance of improved audit performance—a key component, along with improved audit performance and visibility, of any centralized access governance suite. These features reduce complexity and limit associated costs by providing an approach that can be quickly implemented and efficiently automated.

Managing user access through a unified IAG framework has many benefits. The user-friendly approach simplifies the certification process and allows users to edit certain elements of their identities; request roles and entitlements; and manage passwords. Moreover, automated lifecycle event management based on established business policies for user-access privileges frees IT to tackle more important tasks.

As organizations evaluate various approaches to achieve optimal IAG control, from manual “home-brew” and ad-hoc technologies to automation, it is expected that they will increasingly choose suite-based solutions. Such solutions offer increased integration with preexisting processes; scalability and management controls; and lower costs.

Business benefits include dashboards that offer data analysis via graphs, charts, and reports, as well as advanced analytics that can be applied to predefined or custom reports. Streamlined integration and the improved quality of information ensure that business professionals and the IT department aren’t working at cross-purposes. This clear division of responsibility means that business leaders can focus on compliant business processes with the knowledge that resource connectivity is assured.

NetIQ Access Governance Suite

NetIQ Access Governance Suite is an innovative identity and access governance solution that reduces the cost and complexity of complying with regulations and providing access to users. It centralizes identity data, captures business policy, models roles, and proactively manages user and resource risk factors. Rich integration with industry-acclaimed Identity Manager from NetIQ provides a complete IAG solution with trusted fulfillment.

Global accounting giant Mazars recently turned to NetIQ for help in unifying its diverse European workforce, spread across France, the Netherlands, and Great Britain. The company needed to synthesize disparate IAG security controls, including some that were applied manually.

NetIQ, which understood the need to build upon Mazars’ preexisting solutions, used Access Governance Suite along with Identity Manager to unify the company’s diverse security system and synchronize access data across each of its agencies.

Conclusion

To truly protect information assets from security threats and breaches, enforce corporate policies, and meet compliance requirements, organizations today must expand their approach to identity management and consider identity and access governance solutions.

NetIQ Access Governance Suite along with Identity Manager provide a comprehensive IAG solution capable of addressing risk and compliance concerns around accessing applications and sensitive data by applying strong, consistent controls across the enterprise. Ultimately, NetIQ’s IAG solution helps businesses cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly distributed business applications.

For more information, please visit
www.netiq.com