Identity Governance is often implemented as a reaction to demands from auditors. While important, it is short-sighted to look at governance as merely a means to pass audits. Failure to effectively govern user access to sensitive resources places organizations at risk for sabotage, fraud, data breaches and financial penalties.

Today’s attackers are targeting insider credentials for abuse. According to the 2016 Verizon Data Breach Investigations Report, 63% of confirmed data breaches involved weak, default or stolen passwords in the previous year. Even with an effective program in place, there are loopholes that can be exploited by attackers in the way that identity governance is typically implemented in most organizations today.

Managing access risk requires an organization to inventory, analyze and understand the access privileges granted to its workers, and to answer the critical question on demand: “Who has access to what, what are they doing with that access, and is it appropriate?”

An effective identity governance program can do far more than just inventory and certify access—it can be a tool to minimize risk and strengthen your overall security posture as well, if you can close the loopholes.

The Loopholes in Today’s Approach to Identity Governance
Understanding the limitations of current approaches to Identity Governance is the first step to minimizing risk.

- **Business Apathy**: Business managers simply don’t care much about compliance or security, yet we are placing the burden of risk management on them when we ask them to certify access. The result is rubber-stamped approvals that leave an expanded vulnerability footprint.

When employees take on new roles there is often privilege creep—lingering access to resources or data that the individual no longer requires. There are also orphaned accounts that don’t seem to belong to anyone in particular. It is easier for an attacker to abuse insider credentials when those privileges aren’t being regularly used.

- **Tunnel Vision on Compliance** It creates a false sense of security to get an approval from audit. But compliance should be an outcome of good security, not a means to an end. Just because a user has appropriate access rights doesn’t mean they won’t abuse them.
The result is unforeseen risk exposure from legitimate users who could misuse or mistakenly expose their privileges. Or more likely, outside attackers who are constantly working to obtain legitimate credentials through social engineering, phishing attacks or malware downloaded from web pages, with the intent of exploiting those credentials to steal data. This is what happened in the Anthem, Target, OPM and many other high-profile attacks.

- **Blind Spots Created by Point-in-Time Access Certifications:** If access reviews are performed every six to 12 months, as is common in most organizations, what happens in-between the reviews? People change roles or leave the organization. Projects end. Yet those privileges remain longer than is necessary, even if good certifications result in accurate revocations every six months. The result is large windows of time for an attacker to exploit a compromised account.

In order to close these loopholes, identity governance must become far more dynamic. The future of effective identity governance is one that needs to provide better contextual information for business managers at the point of certifying access, such as highlighting orphan accounts, so that rubber-stamping is reduced. It includes information about what users are doing with their access, with abnormal activity exposed and risk scoring to support better decision making. And it includes adaptive certifications that ask a manager to review entitlements when risky behavior occurs, to eliminate blind spots in-between certifications.

**Things to Look for in an Adaptive Identity Governance Solution**

Identity governance solutions should offer capabilities that both address compliance challenges and lower risk. Look for the following capabilities:

- Automated processes for user onboarding, transferring, promoting and terminating, in addition to customizable approval workflows.
- An Identity and Entitlement Catalog that automatically maintains a core set of identities and their relationships to your organization. It should eliminate improper updates from non-authoritative sources and update in near-real time.
- An authorization model that leverages both roles and broader attributes to automate basic approvals for access requests and certifications and allows a focus on exceptions.
- Automated controls for reducing risk, combined with advanced risk analytics to measure baseline risk and the effectiveness of automated controls in reducing risk.
- Controls to detect and handle violations and exceptions, especially SOD conflicts, expired exceptions and orphan or shared accounts.
- An intuitive user experience with mechanisms to close the loop, so access requests and revocations get fulfilled accurately.
- Out-of-the box and ad-hoc compliance reports to demonstrate the program to auditors with minimal effort.

To learn more about Identity Governance, please visit the NetIQ® Identity Governance page at: [www.netiq.com/governance](http://www.netiq.com/governance)