SailPoint

SOLUTION BRIEF

The Importance of Identity Governance to M&A Success

Companies today undergo frequent mergers and acquisitions. Since 2000, more than 790,000 transactions have occurred across the globe, valued at more than $58 trillion[1]. The number of deals and the average size of their transactions will only continue to grow as mergers and acquisitions promise to bring companies into new geographies, accelerate time to market, as well as enable them to offer customers additional products, services and technologies. Yet while M&As deliver significant opportunities for business transformation, the necessary investment and business impacts can lead to the most substantial challenges an organization may ever face.

Key components of a successful merger or acquisition include planning and executing critical Day 1 access, ensuring effective integrations and accelerating the monetization of your investment. Yet the logistics of joining two companies can be daunting. Among the biggest undertakings is ensuring that employees can perform their jobs productively from Day 1. Every day that employees are unable to access their software applications, data and IT systems significantly reduces ROI from the merger or acquisition. Properly granting Day 1 access is critical for fostering employee productivity, profitability and customer retention. At the same time, companies must comply with policies and regulations regarding who can access what data while properly securing personal and confidential information from unauthorized access.

Corporations and private equity firms say that effective integration is the single most important contributor to a successful transaction.[2]

Organizations that are the most successful at traversing these tasks have found that identity governance is a key lynchpin for their M&A IT strategy. Utilizing a modern, predictive identity governance solution that incorporates artificial intelligence and machine learning while supporting cloud-first initiatives can significantly reduce time, cost and effort while accelerating return on investment. Pre-merger, identity governance enables you to define roles and access privileges for different users,

[1] https://imaa-institute.org/mergers-and-acquisitions-statistics/
[2] "The State of the Deal: M&A Trends Report 2019," Deloitte

departments, locations and job functions and get a complete view of all users and their current access. On Day 1, you can automatically onboard up to thousands of new users, rapidly giving them access to the systems they need. After Day 1, you can easily demonstrate to auditors that access has been granted or terminated in accordance with compliance regulations.

The following explains how identity governance supports your organization throughout the merger or acquisition process while ensuring compliance and strengthened IT security:

Ensuring a Successful Day 1

Ensuring that workers are up and running on Day 1 starts long before the merger is finalized. Your organization can jump start the process by defining roles and associated access privileges for different users, departments, locations, job functions and more. Today, many organizations use slow, error-prone manual processes or spreadsheets to determine who should have access to what and then verify this information with line-of-business managers. If you are dealing with thousands of users, this can be an overwhelming, unwieldy task. The power of artificial intelligence greatly simplifies and speeds up the process of defining access models and roles. Identity governance also gives you a 360-degree view of users, groups, and their related access pre-merger, slashing Day 1 planning from weeks to days.

56%

of U.S. executives say they are starting integration earlier in the M&A process.[3]

Once Day 1 of the merger arrives, you need to quickly get new users up and running on the most essential systems such as HR, Active Directory, email, and important financial applications. By using an identity governance solution, you can accelerate and automate onboarding processes that deliver access for hundreds or thousands of users to the applications, systems and data they need--including cloud file storage locations such as Box, Drobox and SharePoint. In addition, automated offboarding processes ensure that access for terminated employees is completely removed and documented.

After initial user access is granted, self-service capabilities enable employees to reset passwords and request access -- which can be fulfilled according to organizational policies -- all without costly calls to the IT helpdesk. When users request access, AI-driven identity helps to provide recommendations of whether access should or should not be approved helping organizations make rapid, intelligent access decisions.

[3] "Capital Confidence Barometer," EY

Once your Day 1 transition is complete, your IT department can then focus on prioritizing and onboarding applications from the acquired company into your identity governance program and ensuring the right users and groups have access to them.

Confident and Continuous Compliance

Companies undergoing mergers/acquisitions must ensure compliance with regulations such as the Sarbanes-Oxley Act (SOX) of 2002. Designed to protect investors and bolster the trustworthiness of corporate financial statements, SOX requires auditors and corporate executives to detect fraud and external threats. Public companies must perform internal controls tests and provide audit trails of all access and activity to sensitive business information.

To ensure compliance, you must:

- Govern access to PII and sensitive data consistently across the organization, including human and non-human access such as software bots
- Document your access controls
- Periodically certify user access to monitor for changes

Identity governance enables SOX compliance by allowing you to take your 360 view of all users and apply appropriate access models and policies to ensure the right users have access to the right resources – such as applications, cloud infrastructure, privileged accounts and data files.

Additionally, identity governance helps prevent toxic combinations of access by enforcing separation of duties to avoid fraud and conflicts of interest. With access appropriately assigned, identity governance monitors and documents all access activity in the form of an audit trail, which can be used to demonstrate compliance to auditors post-merger. To maintain ongoing compliance, you should perform periodic and ad hoc access reviews and certifications to identify and remediate compliance gaps.

Identity governance enables you to rest assured—and demonstrate—that you meet SOX standards and other regulations as you embark on your merger or acquisition and also successfully maintain controls as the two organizations combine operations.

Protect Against M&A Security Risks

Cybersecurity risk is an important though often overlooked consideration for companies undergoing mergers and acquisitions. A recent survey of 100 senior global executives found that 52 percent reported discovering a cybersecurity problem after closing the deal[4]. A breach in an acquired company due to inadequate security controls can leave the acquiring company liable for damages.

[4] https://www.darkreading.com/application-security/security-matters-when-it-comes-to-mergers-and-acquisitions/a/d-id/1333548

To protect your organization from financial implications or reputational compromise that often arise from data breaches, organizations must vet cybersecurity controls for companies they are acquiring or merging with before the deal is signed. According to Gartner[5], your due diligence process must include reports and documentation such as vulnerability assessments, penetration testing, security controls as well as documentation or certifications related to security functions. This information will help you understand current risk levels and prepare for post-close.

Once Day 1 arrives, identity governance allows you to get a clear view of all user access to all applications and files across a hybrid infrastructure. Using a predictive identity approach, artificial intelligence enables your IT department to analyze peer groups and quickly identify risky outliers that may be over permissioned or possess questionable access. You can then perform ad-hoc access reviews and certifications on these outliers to verify whether access is appropriate and adjust accordingly.

To enhance ongoing security and minimize risk, identity governance helps ensure that every new or existing user has only the access privileges necessary to do their job. When users change roles or job functions, or leave the organization, access is automatically adjusted. Additionally, using artificial intelligence and machine learning, predictive identity enables you to continuously monitor and remediate anomalous access activity arising from internal or external threats.

Finally, when workers are terminated, it is important to ensure that all access is removed. An alarming report on insider threats estimated that over 1/3 of employees continued to have access to systems or data from an employer after they left a job[6]. Identity governance helps automatically remove all access and disable user accounts, ensuring that these users no longer have access to the IT infrastructure.

Efficient Divestitures

Not only does identity governance play a key role in successful mergers and acquisitions, it is also called upon when organizations are required to divest a portion of their business. A complete view of all users and their current access can be used to pre-plan access rights for users being spun off, those staying with the company or users being terminated. On Day 1, automation facilitates the offboarding of users from the parent organization, ensuring access is provisioned as part of their new organization or completely removed in the case where they are no longer continuing employment. All activity is then documented and can be used to demonstrate compliance to auditors.

[5] "Cybersecurity is Critical to the M&A Due Diligence Process," Gartner
[6] https://www.isdecisions.com/insider-threat-persona-study/

Conclusion

Mergers and acquisitions promise enormous benefits that can include expanding into new geographic markets and growing product and service offerings. But returns and profitability for an M&A can easily be derailed if employees are unable to access the enterprise applications, systems and data they need to hit the ground running on Day 1.

Comprehensive identity governance gives you complete visibility and control over access across all stages of the M&A process, enabling consistent employee onboarding and helping you reduce the time, cost and effort involved. In particular, identity governance enables you to:

- Plan integration strategies before the merger by understanding all users and their access to applications, systems, cloud infrastructure and data files
- Accelerate time to value by provisioning and deprovisioning IT access automatically for hundreds to thousands of users on Day 1
- Automatically and simultaneously shut off access for those workers not continuing employment
- Reduce IT burden and costs by giving employees self-service capabilities for requesting access and managing passwords
- Quickly onboard and centrally manage applications and files from the acquired company and ensure the right users and groups can access them
- Ensure ongoing regulatory compliance by creating, enforcing and documenting user access policies, auditing user access activity, and performing ongoing access reviews and certifications
- Strengthen cybersecurity by monitoring and remediating anomalous access activity
- Remain in compliance during divestitures by ensuring that employees are offboarded properly

Enterprises around the world rely on SailPoint Predictive Identity to prepare for and execute a successful Day 1 – and beyond. As a leader in identity, SailPoint is poised to help IT enable the M&A transaction, ensuring your business operates without disruption by providing a smooth transition, continuous compliance and enhanced security across your newly blended organization.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1338-2002