

# Die Bedeutung von Identity Governance für erfolgreiche M&A-Prozesse



Unternehmen erleben heutzutage öfter Fusionen und Übernahmen. Seit 2000 erfolgten weltweit mehr als 790.000 Transaktionen im Wert von über 58 Bio. USD<sup>1</sup>. Da Fusionen und Übernahmen Unternehmen die Expansion in neue Märkte, eine kürzere Amortisierungszeit und die Möglichkeit, Kunden zusätzliche Produkte, Services und Technologien anzubieten, ermöglichen, wird die Anzahl der Deals und die durchschnittliche Höhe der Transaktionen immer weiter steigen. Doch während M&As (Mergers & Acquisitions; Fusionen und Übernahmen) beträchtliche Möglichkeiten für eine Geschäftsumgestaltung bieten, können die erforderlichen Investitionen und die resultierenden Geschäftsauswirkungen zu den einschneidendsten Herausforderungen führen, vor denen ein Unternehmen während seines Bestehens steht.

Zu den wichtigsten Komponenten einer erfolgreichen Fusion oder Übernahme zählen die Planung und Ausführung von entscheidenden Zugriffsrechten an Tag 1, wodurch eine effektive Integration sichergestellt und die Monetarisierung Ihres Investments beschleunigt wird. Doch die logistische Aufgabe, zwei Unternehmen zusammenzuführen, kann entmutigen. Eines der wichtigsten Unterfangen ist, sicherzustellen, dass die Mitarbeiter vom ersten Tag an produktiv ihre Arbeit erledigen können. Jeder Tag, an dem Mitarbeiter nicht auf Software, Daten und IT-Systeme zugreifen können, reduziert den ROI der Fusion oder Übernahme signifikant. Die korrekte Gewährung von Zugriff ab Tag 1 ist ausschlaggebend für die Förderung der Mitarbeiterproduktivität, der Profitabilität und der Kundenbindung. Zur selben Zeit müssen Unternehmen die Richtlinien und Regelungen für den Zugriff auf ihre Daten einhalten wie auch persönliche und vertrauliche Daten vor nicht autorisiertem Zugriff schützen.



**Unternehmen und Privatkapitalgesellschaften geben an, dass eine effektive Integration der wichtigste Faktor für eine erfolgreiche Transaktion ist.<sup>2</sup>**

<sup>1</sup> <https://imaa-institute.org/mergers-and-acquisitions-statistics/>

<sup>2</sup> „The State of the Deal: M&A Trends Report 2019“, Deloitte

Organisationen, die diese Aufgabe am erfolgreichsten bewältigt haben, stellten fest, dass Identity Governance das Kernelement ihrer IT-Strategie bei einer Fusion oder Übernahme war. Der Einsatz einer modernen Lösung für Predictive-Identity-Governance, die künstliche Intelligenz und maschinelles Lernen einschließt und Cloud-basierte Initiativen unterstützt, kann den Zeit-, Kosten- und Arbeitsaufwand signifikant reduzieren und die Rendite antreiben. Identity-Governance noch vor der Fusion ermöglicht Ihnen, Rollen und Zugriffsberechtigungen für verschiedene Nutzer, Abteilungen, Standorte und Arbeitsaufgaben zu definieren und eine Gesamtansicht aller Nutzer und ihrer aktuellen Zugriffsrechte zu erhalten. An Tag 1 können Sie automatisch bis zu Tausende von Nutzern eingliedern und ihnen umgehend Zugriff auf die erforderlichen Systeme gewähren. Anschließend können Sie Auditoren auf einfache Weise aufzeigen, dass Zugriff gemäß der Compliance-Vorschriften gewährt oder entzogen wurde.

Im Folgenden wird aufgezeigt, wie Identity Governance Ihre Organisation während des gesamten Verlaufs der Fusion oder Übernahme unterstützt und gleichzeitig Compliance sichergestellt und die IT-Sicherheit gestärkt wird:

### Sicherstellung eines erfolgreichen Tages 1

Um sicherstellen zu können, dass die Mitarbeiter ihre Tätigkeit vom ersten Tag an ausführen können, muss schon lange vor der Finalisierung der Fusion mit der Planung begonnen werden. Ihre Organisation kann sich einen Vorsprung in diesem Prozess sichern, indem Sie Rollen und zugeordnete Zugriffsberechtigungen für verschiedene Nutzer, Abteilungen, Standorte und Arbeitsaufgaben definieren. Viele Organisationen setzen heute langsame und fehleranfällige, manuelle Prozesse oder Tabellenblätter ein, um zu ermitteln, wer auf was Zugriff haben sollte, und diese Informationen dann mit Line of Business Managern zu verifizieren.

Wenn Sie jedoch Tausende von Nutzern haben, kann dies eine überwältigende, unübersichtliche Aufgabe sein. Die Power der künstlichen Intelligenz vereinfacht und beschleunigt das Definieren von Zugriffsmodellen und Rollen beträchtlich. Mit Identity Governance erhalten Sie außerdem einen Rundumeinblick in Nutzer, Gruppen und ihren Zugriff vor der Fusion, wodurch die Planung für Tag 1 nicht mehr Wochen, sondern Tage in Anspruch nimmt.



**56 %**

der US-Führungskräfte geben an, dass sie im M&A-Prozess früher mit der Integration beginnen.<sup>3</sup>

Wenn Tag 1 schließlich eintritt, müssen Sie neuen Benutzern so schnell wie möglich den Zugriff auf essentielle Systeme wie das Personalsystem, Active Directory, E-Mails und wichtige Finanzanwendungen gewähren. Durch den Einsatz einer Identity Governance-Lösung können Sie Onboarding-Prozesse beschleunigen und automatisieren, um Hunderten oder Tausenden Nutzern schnell Zugriff auf die Anwendungen, Systeme und Dateien zu gewähren, die sie für ihre Arbeit benötigen, darunter auch Cloud-Dateispeicherstandorte wie Box, Dropbox und SharePoint. Außerdem stellen automatisierte Offboarding-Prozesse sicher, dass der Zugriff ausscheidender Mitarbeiter komplett aufgehoben und dokumentiert wird.

<sup>3</sup> „Capital Confidence Barometer“, EY

Wurde den Nutzern der Zugriff gewährt, können sie dank der Self-Service-Fähigkeiten und entsprechend der Organisationsrichtlinien eigenständig Zugriffsanforderungen stellen und Passwörter zurücksetzen, ganz ohne kostspielige IT-Helpdeskanrufe. Bei Zugriffsanfragen durch Nutzer spricht die KI-gestützte Identity Empfehlungen aus, ob der Zugriff gewährt werden sollte oder nicht, sodass Organisationen Zugriffsentscheidungen schnell und intelligent treffen können.

Sobald die Umstellung an Tag 1 abgeschlossen wurde, kann sich Ihre IT-Abteilung darauf konzentrieren, die Anwendungen der erworbenen Firma in Ihr Identity Governance-Programm einzugliedern und sicherzustellen, dass die richtigen Nutzer und Gruppen darauf zugreifen können.

### Zuverlässige und kontinuierliche Compliance

Unternehmen, die vor einer Fusion oder Übernahme stehen, müssen die Einhaltung von Regelungen wie dem Sarbanes-Oxley Act (SOX) von 2002 sicherstellen. Der SOX Act soll Investoren schützen und die Vertrauenswürdigkeit von Geschäftsberichten untermauern und erfordert von Auditoren und der Konzernführung, Betrug und externe Bedrohungen aufzudecken. Aktiengesellschaften müssen dabei interne Kontrolltests ausführen und Audit-Trails aller Zugriffe und Aktivitäten in Bezug auf sensible Geschäftsinformationen bereitstellen.

#### Um Compliance sicherzustellen, müssen Sie:

- Den Zugriff auf personenbezogene und sensible Daten organisationsweit einheitlich regeln, einschließlich menschlicher und nicht-menschlicher Zugriff, zum Beispiel durch Software-Bots
- Ihre Zugriffskontrollen dokumentieren
- Den Nutzerzugriff periodisch zertifizieren, um Änderungen zu berücksichtigen

Identity Governance ermöglicht die Compliance mit dem SOX Act, indem es Ihnen eine Rundumansicht aller Nutzer und die Anwendung entsprechender Zugriffsmodelle und -richtlinien erlaubt, mit denen Sie sicherstellen können, dass die richtigen Nutzer Zugriff auf die richtigen Ressourcen haben, darunter Anwendungen, Cloud-Infrastruktur, privilegierte Konten und Dateien.

Identity Governance beugt außerdem toxische Zugriffskombinationen und somit Missbrauch und Interessenskonflikte vor, indem eine Aufgabentrennung erzwungen wird. Nach der ordnungsgemäßen Zugriffszuweisung überwacht und dokumentiert Identity Governance sämtliche Zugriffsaktivitäten in Form eines Audit-Trails, über den Auditoren nach der Fusion Compliance demonstriert werden kann. Um kontinuierliche Compliance sicherzustellen, sollten Sie periodische sowie Ad-hoc-Zugriffsüberprüfungen und -Zertifizierungen ausführen, um Compliance-Lücken zu identifizieren und zu beheben.

Mit Identity Governance können Sie sicher sein und nachweisen, dass Sie SOX-Standards und andere Bestimmungen einhalten, während Sie Ihre Fusion oder Übernahme abwickeln, und erfolgreich die Kontrolle behalten, während die Betriebsabläufe der beiden Organisationen zusammengeführt werden.

## Schutz vor Sicherheitsrisiken bei Fusionen und Übernahmen

Cybersicherheitsrisiken sind ein wichtiges zu berücksichtigendes Element für Unternehmen, die eine Fusion oder Übernahme erleben. Eine aktuelle Umfrage unter 100 globalen Führungskräften kam zu dem Ergebnis, dass 52 Prozent nach Abschluss des Deals ein Cybersicherheitsproblem erkannten<sup>4</sup>. Ein Richtlinienverstoß durch ein erworbenes Unternehmen aufgrund inadäquater Sicherheitskontrollen kann das erwerbende Unternehmen schadensersatzpflichtig machen.

Um Ihre Organisation vor finanziellen Auswirkungen oder einer Beeinträchtigung der Reputation zu schützen, welche Datenschutzverletzungen oftmals mit sich bringen, müssen Organisationen die Cybersicherheitskontrollen der Unternehmen, die sie erwerben oder mit denen sie fusionieren, vor Unterzeichnung des Deals überprüfen. Laut Gartner<sup>5</sup> muss Ihr Due-Diligence-Prozess Berichte und Dokumentation wie Schwachstellenanalysen, Penetrationstests, Sicherheitskontrollen sowie Dokumentation oder Zertifizierungen hinsichtlich Sicherheitsfunktionen beinhalten. Diese Informationen helfen Ihnen dabei, das aktuelle Risikoniveau nachzuvollziehen und sich auf die Zeit nach der Abschließung vorzubereiten.

Ab Tag 1 ermöglicht Ihnen Identity Governance, einen klaren Überblick über den Nutzerzugriff auf sämtliche Anwendungen und Dateien einer Hybrid-Infrastruktur zu erhalten. Durch einen Predictive Identity-Ansatz kann Ihre IT-Abteilung dank der künstlichen Intelligenz Peergruppen analysieren und schnell riskante Ausreißer identifizieren, die überberechtigt sind oder fragwürdige Zugriffsrechte haben. Sie können für diese Ausreißer dann Ad-hoc-Zugriffsprüfungen und -Zertifizierungen ausführen, um zu verifizieren, ob der Zugriff angemessen ist, und entsprechende Anpassungen vornehmen.

Um die laufende Sicherheit zu verbessern und Risiken zu minimieren, stellt Identity Governance sicher, dass jeder neue oder existierende Nutzer nur über die Zugriffsberechtigungen verfügt, die er für seine Arbeit benötigt. Wenn sie ihre Rollen oder Arbeitsaufgaben wechseln oder das Unternehmen verlassen, wird ihr Zugriff automatisch angepasst. Durch den Einsatz von künstlicher Intelligenz und maschinellem Lernen ermöglicht es Ihnen Predictive Identity außerdem, anomale Zugriffsaktivitäten, die sich aus internen oder externen Bedrohungen ergeben, kontinuierlich zu überwachen und zu beheben.

Schließlich ist es wichtig, dass sämtliche Zugriffsberechtigungen entzogen werden, wenn ein Mitarbeiter das Unternehmen verlässt. Ein bedenklicher Bericht zum Thema interne Bedrohungen kam zu dem Ergebnis, dass geschätzt ein Drittel aller Mitarbeiter weiterhin Zugriff auf Systeme oder Daten eines Arbeitgebers haben, nachdem sie ein Unternehmen verlassen haben<sup>6</sup>. Mit Identity Governance können automatisch sämtliche Zugriffsberechtigungen entzogen und Nutzerkonten deaktiviert werden, sodass die entsprechenden Nutzer nicht mehr auf die IT-Infrastruktur zugreifen können.

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

<sup>5</sup> „Cybersecurity is Critical to the M&A Due Diligence Process“, Gartner

<sup>6</sup> <https://www.isdecisions.com/insider-threat-persona-study/>

## Effiziente Veräußerungen

Identity Governance spielt nicht nur bei Fusionen und Übernahmen eine Schlüsselrolle, sondern wird auch eingesetzt, wenn Organisationen einen Anteil ihres Geschäfts veräußern müssen. Eine Gesamtansicht aller Benutzer und ihrer Zugriffsberechtigungen kann dabei helfen, Zugriffsrechte für ausgegliederte, verbleibende oder gekündigte Nutzer im Voraus zu planen. An Tag 1 erleichtert die Automatisierung das Offboarding von Nutzern der Ursprungsorganisation, wodurch sichergestellt wird, dass der Zugriff als Teil ihrer neuen Organisation gewährt oder komplett entfernt wird, wenn sie aus dem Unternehmen ausscheiden. Sämtliche Aktivitäten werden dokumentiert und können zur Compliance-Demonstration Auditoren vorgelegt werden.

## Schlussfolgerung

Fusionen und Übernahmen versprechen enorme Vorteile, wie zum Beispiel die Expansion in neue Märkte sowie ein wachsendes Produkt- und Service-Angebot. Der Ertrag und die Rentabilität einer Fusion oder Übernahme können jedoch leicht gefährdet werden, wenn Mitarbeiter nicht auf die Anwendungen, Systeme und Daten zugreifen können, die sie benötigen, um an Tag 1 durchzustarten.

Umfassende Identity Governance ermöglicht Ihnen völlige Transparenz und Kontrolle über den Zugriff bei allen Stufen des M&A-Prozesses. So profitieren Sie von einem einheitlichen Mitarbeiter-Onboarding mit reduzierten Kosten und Aufwand. Identity Governance ermöglicht Ihnen insbesondere:

- Planung von Integrationsstrategien vor der Fusion durch das Nachvollziehen aller Nutzer und ihres Zugriffs auf Anwendungen, Systeme, Cloud-Infrastrukturen und Dateien
- Beschleunigung der Amortisierungszeit durch automatisches Bereitstellen und Entziehen von IT-Zugriff für Hunderte oder gar Tausende von Nutzern bereits ab Tag 1
- Automatisches und simultanes Entziehen von Zugriffsrechten bei ausscheidenden Mitarbeitern
- Reduzierung des IT-Aufwands und der Kosten, indem Sie Mitarbeitern die Möglichkeit bieten, selbst Zugriffsanfragen zu stellen und Passwörter zu verwalten
- Schnelles Onboarding und zentrale Verwaltung von Anwendungen und Dateien der erworbenen Firma und Sicherstellung, dass die richtigen Nutzer und Gruppen darauf zugreifen können
- Sicherstellung anhaltender Einhaltung der Vorschriften durch die Erstellung, Durchsetzung und Dokumentation von Nutzerzugriffsrichtlinien, die Überprüfung von Zugriffsaktivitäten und die Ausführung von Zugriffsüberprüfungen und Zertifizierungen
- Stärkung der Cybersicherheit durch das Überwachen und Beseitigen anomaler Zugriffsaktivitäten
- Andauernde Compliance auch bei Veräußerungen, indem sichergestellt wird, dass Mitarbeiter-Offboarding ordnungsgemäß erfolgt

Unternehmen auf der ganzen Welt verlassen sich auf SailPoint Predictive Identity für die Vorbereitung und Ausführung eines erfolgreichen Tag 1 und darüber hinaus. Als führender Spezialist im Bereich Identity ist SailPoint der ideale Partner für IT-Abteilungen bei der Ausführung einer Fusion oder Übernahme und stellt sicher, dass Ihr Unternehmen dank eines reibungslosen Übergangs, kontinuierlicher Compliance und einer erhöhten Sicherheit in Ihrer gesamten, frisch fusionierten Organisation unterbrechungsfrei agieren kann.

---

**SAILPOINT:  
RETHINK  
IDENTITY**

**[sailpoint.com](https://sailpoint.com)**

SailPoint, der führende Spezialist für Identity Management, verfolgt einen innovativen Ansatz bei der unternehmensweiten Sicherung des Zugriffs mithilfe der SailPoint Predictive Identity™ Plattform. Dank SailPoint können Unternehmen auf intuitive Weise automatisch sicherstellen, dass jeder Nutzer den für ihn passenden Zugriff zum richtigen Zeitpunkt hat. Angetrieben von patentierter Künstlicher Intelligenz (KI) und maschinellem Lernen (ML) hat die SailPoint Predictive Identity™ Plattform das Ziel, den Betrieb auf sichere Weise zu beschleunigen und gleichzeitig adaptive Sicherheit, kontinuierliche Compliance und eine verbesserte Geschäftseffizienz sicherzustellen. Als Pionier und Marktführer im Bereich Identity Governance, zu dessen Kunden einige der weltweit bekanntesten Unternehmen zählen, treibt SailPoint die Branche konsequent dazu an, Identity zum Vorteil der dynamischen Geschäftsbedürfnisse der Kunden neu zu überdenken.

Folgen Sie SailPoint auf [Twitter](#) und [LinkedIn](#) um auf dem Laufenden zu sein und abonnieren Sie den [SailPoint blog](#).