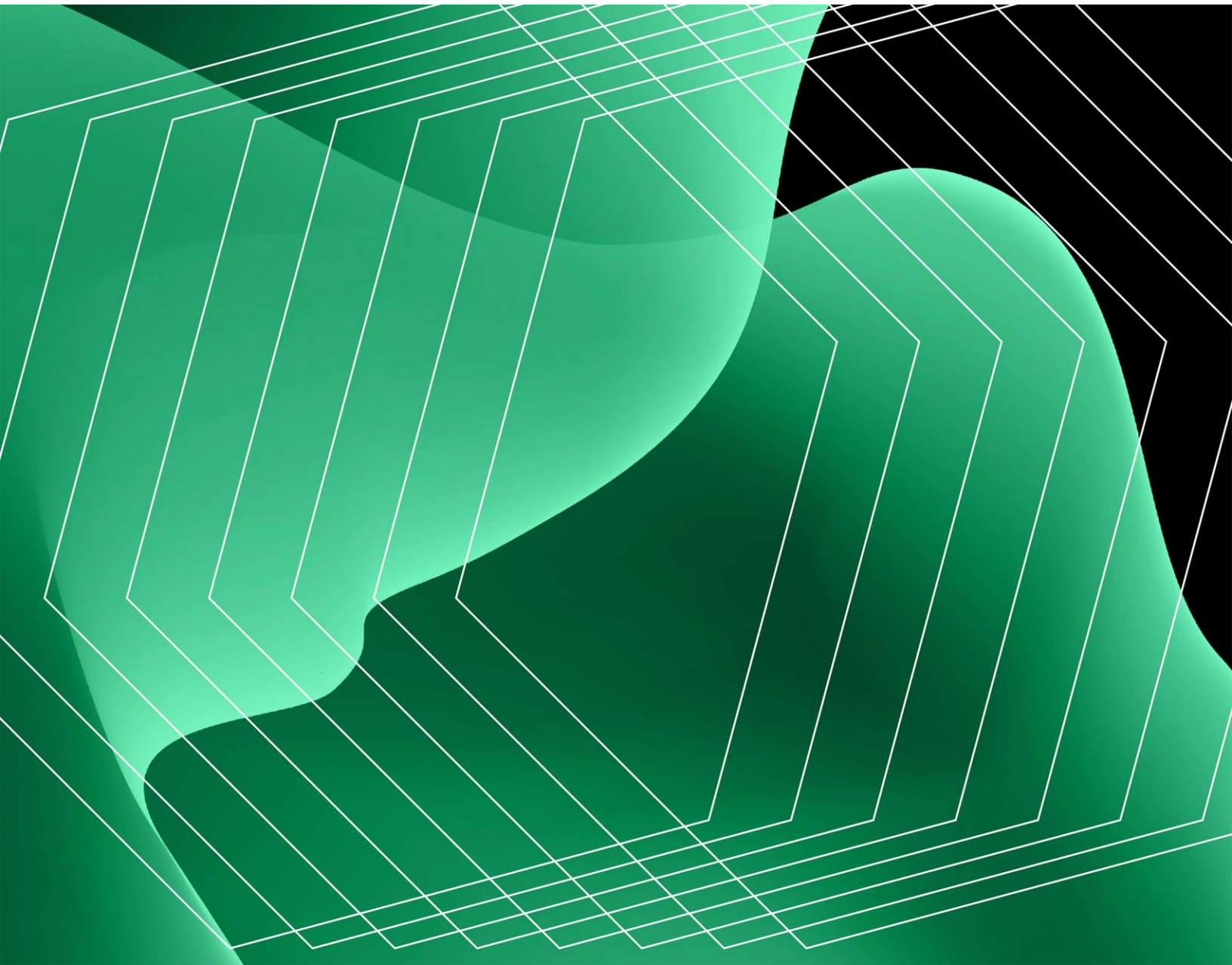
FORRESTER®

Der Total Economic Impact™ von Okta Identity Governance

Kosteneinsparungen und geschäftlicher Nutzen durch Identity Governance

EINE FORRESTER TOTAL ECONOMIC IMPACT-STUDIE
IM AUFTRAG VON OKTA, JUNI 2025



Inhaltsverzeichnis

Beraterteam:

Kris Peterson

ÜBER FORRESTER CONSULTING

Forrester bietet unabhängige, objektive und auf Forschungsergebnisse gestützte Beratungsdienstleistungen und unterstützt Führungskräfte beim Erreichen ihrer Ziele. In kundenfokussierten Studien arbeiten die erfahrenen Beraterinnen und Berater von Forrester gemeinsam mit Führungskräften daran, deren spezifische Prioritäten umzusetzen. Dabei kommt ein spezielles Kooperationsmodell zum Einsatz, das eine nachhaltige Wirkung sicherstellt. Weitere Informationen erhalten Sie unter forrester.com/consulting.

Zusammenfassung

Unternehmen aller Größen benötigen einen proaktiven, richtliniengesteuerten Ansatz für die Zugriffs- und Berechtigungsverwaltung. Angesichts zunehmender Sicherheitsbedrohungen und regulatorischer Vorgaben wie SOX und PCI-DSS gilt es dabei, die goldene Mitte zwischen Flexibilität und Skalierbarkeit auf der einen und Kontrolle, Aufsicht und Compliance auf der anderen Seite zu finden. Unterschiedliche Systeme und manuelle Prozesse erzeugen häufig blinde Flecken und verzögern die Bereitstellung des Zugriffs. Außerdem müssen in solchen Konstellationen Anwender mit zu vielen Berechtigungen umgehen und das Reporting wird sehr zeitaufwendig. Da Identitätsumgebungen immer größer und komplexer werden, brauchen Unternehmen Governance-Lösungen, die in die zentrale Identitätsinfrastruktur integriert werden können, um sowohl die betriebliche Effizienz als auch die Risikominimierung zu unterstützen.

Okta Identity Governance (OIG), eine cloudbasierte Lösung für Identity Governance und Identitätsverwaltung (Identity Governance and Administration, IGA), kann direkt in die Identitätsinfrastruktur integriert werden. So lassen sich Zugriffsanforderungen, Zertifizierungen, Berechtigungsüberprüfungen, die Richtliniendurchsetzung und das Reporting zentralisieren und automatisieren. OIG ersetzt manuelle Arbeitsabläufe durch ereignisgesteuerte Automatisierungen und eine dynamische Zugriffslogik. Unternehmen können auf diese Weise den Zugriff nach dem Least-Privilege-Prinzip durchsetzen, die Bereitstellung und ihre Aufhebung beschleunigen und die Compliance in großem Umfang sicherstellen – und gleichzeitig den Verwaltungsaufwand und Zugriffsrisiken verringern.

Okta beauftragte Forrester Consulting mit der Durchführung einer Total Economic Impact™ (TEI)-Studie sowie mit der Untersuchung des potenziellen Return on Investment (ROI), den Unternehmen durch den Einsatz von Okta Identity Governance erzielen können.[1] Ziel dieser Studie ist es, den Lesern eine Rahmenstruktur zur Beurteilung der potenziellen finanziellen Auswirkungen von Okta Identity Governance auf ihr jeweiliges Unternehmen bereitzustellen.

Kapitalrendite (ROI)
211 %

Kapitalwert
1,8 Mio. $

Um die mit dieser Investition verbundenen Vorteile, Kosten und Risiken besser zu verstehen, befragte Forrester acht Verantwortliche, die bereits Erfahrung mit OIG haben. Die Erfahrungen der befragten Personen wurden von Forrester für diese Studie zusammengefasst und als Grundlage zur Erstellung eines einzigen Modellunternehmens verwendet. Bei diesem Modellunternehmen handelt es sich um ein globales Unternehmen mit einem Jahresumsatz von 1,5 Mrd. USD, 5.000 Identitäten, 100 Anwendungen und 12 Mitarbeitern, die für die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM), die Unterstützung von Audits und die Durchsetzung der Compliance verantwortlich sind.

Nach Angaben der Befragten waren ihre Umgebungen vor der Implementierung von OIG in hohem Maße von manuellen Aufgaben, fragmentierten Tools und inkonsistenten Zugriffsrichtlinien abhängig. Dies führte zu ineffizienten Abläufen, menschlichen Fehlern und Sicherheitslücken. Versuche in der Vergangenheit, die Identity Governance zu formalisieren, waren oft unvollständig oder langfristig nicht umsetzbar. Dies führte zu verspäteter Bereitstellung, Auditproblemen, einem erhöhten Risikopotenzial und gab Anwendern zu viele Berechtigungen.

Nach der Investition in OIG konnten die Befragten einen Übergang von reaktiver Beaufsichtigung hin zu einer proaktiven, richtliniengesteuerten Governance feststellen. Die IAM-Teams profitierten nun von zentraler Transparenz, konnten die wichtigsten Arbeitsabläufe automatisieren und Zugriffskontrollen konsistenter erzwingen – und so nicht nur die Servicebereitstellung beschleunigen, sondern auch Audits vereinfachen und das Sicherheitsniveau erhöhen.

WESENTLICHE ERGEBNISSE

Quantifizierter Nutzen. Für das Modellunternehmen setzt sich der risikobereinigte barwertige Nutzen über den dreijährigen Analysezeitraum folgendermaßen zusammen:

- **Höhere Effizienz bei der Identity Governance im Wert von 1,1 Mio. USD.** Durch die Automatisierung von Zugriffsanforderungen, die Überprüfung von Zertifizierungen und die Berechtigungsverwaltung konnte der Arbeitsaufwand der IAM- und IT-Supportteams des Modellunternehmens um bis zu 60 % gesenkt werden. Diese Einsparungen ergeben sich durch die Reduzierung der manuellen Eingriffe, die für die Zugriffsüberprüfung, die Bereinigung von Berechtigungen und für Ad-hoc-Zugriffsanforderungen erforderlich waren. Außerdem mussten Vorgesetzte weniger Zeit für die Überprüfung und Genehmigung von Zugriffsanfragen aufbringen.
- **Geringerer Aufwand für die Vorbereitung von Audits und das Compliance-Reporting und damit Kosteneinsparungen in Höhe von 232.000 USD.** Dank der höheren

Zugriffstransparenz und der Automatisierung von Überprüfungen wurde die Sammlung von Nachweisen vereinfacht. Gleichzeitig musste das Modellunternehmen weniger Zeit dafür investieren, den internen und externen Auditanforderungen nachzukommen, darunter auch den Anforderungen gemäß SOX, PCI-DSS und anderen regulatorischen Rahmenwerken. Darüber hinaus profitiert das Modellunternehmen von konsistenteren Abläufen bei Zertifizierungen und der Zugriffskontrolle. Dies verhindert schlechte Auditergebnisse und optimiert den allgemeinen Governance-Status.

- **Höhere Plattformeffizienz und Softwarerationalisierung mit daraus folgenden Effizienzgewinnen in Höhe von 567.000 USD.** Das Unternehmen ersetzte veraltete Tools und kostspielige Konnektoren durch vorkonfigurierte Integrationen und erhöhte die Transparenz bei Berechtigungen. Auf diese Weise kann es Lizenz- und Beratungskosten einsparen und gleichzeitig den Verwaltungsaufwand für Onboarding, Offboarding und Zugriffsänderungen reduzieren. Governance-Arbeitsabläufe automatisieren wichtige Joiner-Mover-Leaver-Prozesse und ermöglichen die richtlinienbasierte Durchsetzung, ohne den Personalbedarf zu erhöhen.
- **Steigerung der Produktivität durch Verbesserungen der Zugriffs-Governance, deren Wert auf 497.000 USD beziffert wird.** Endanwender, Vorgesetzte und Anwendungsverantwortliche im Modellunternehmen verbringen weniger Zeit damit, manuelle Genehmigungsketten zu verwalten oder Zugriffsprobleme zu verfolgen. Stattdessen können sie sich auf andere, wertschöpfende Geschäftsaufgaben konzentrieren. Selbst moderate Zeiteinsparungen pro Anwender können bei einer großen Anwenderbasis viel bewirken. Optimierte Anwendererlebnisse und einheitliche, auditgeeignete Arbeitsabläufe minimieren Verzögerungen und erhöhen die geschäftliche Flexibilität.
- **Geringeres Risiko von Sicherheitsverletzungen mit potenziellen Einsparungen von 231.000 USD.** Das Modellunternehmen verringert das messbare Risiko von Sicherheitsverletzungen, indem es seinen Governance-Status verbessert und übermäßige oder veraltete Zugriffsrechte entfernt. Durch die Governance-Automatisierung und proaktive Berechtigungsüberprüfungen wird das Risiko der missbräuchlichen Nutzung von Berechtigungen sowie von internen Bedrohungen verringert. Gleichzeitig ist eine konsistentere Verbreitung von Zugriffsrichtlinien auf allen Systemen möglich.

Nicht quantifizierter Nutzen. Zu den Vorteilen, die einen Wert für das Modellunternehmen darstellen, aber für diese Studie nicht quantifiziert werden, gehören:

- **Kürzere Time-to-Value.** Okta Identity Governance lässt sich im Vergleich zu herkömmlichen IGA-Lösungen schneller bereitstellen. Das Modellunternehmen profitiert vom unmittelbaren Wert der Automatisierung, dem schnelleren Onboarding von Anwendern und Anwendungen und einer besonders kurzen Anlaufzeit und kann damit die Realisierung der quantifizierten Vorteile um mehrere Wochen, wenn nicht sogar Monate, beschleunigen.
- **Verbesserte Arbeitsmoral im IAM-Team.** Die Teams des Modellunternehmens können sich von wiederholten, manuellen Aufgaben der Identity Governance verabschieden und sich stattdessen auf strategische Aktivitäten mit größerer Wertschöpfung konzentrieren, z. B. auf die Definition von Richtlinien, die Ausnahmebehandlung und die Roadmap-Planung.
- **Verbesserung der Mitarbeiter- und Anwendererfahrung.** Endanwender erleben weniger Zugriffsverzögerungen oder -störungen, und Vorgesetzte verbringen weniger Zeit mit der Überprüfung und Genehmigung von Zugriffszertifizierungen und -anforderungen. Mithilfe von Self-Service-Zugriff und optimierten Genehmigungsabläufen reduziert das Modellunternehmen Probleme und optimiert den Zugriff auf geschäftskritische Systeme.

Kosten. Die risikobereinigten barwertigen Kosten über drei Jahre für das Modellunternehmen umfassen:

- **OIG-Lizenzierungsgebühren in Höhe von 821.00 USD.** Diese Summe entspricht den Gesamtkosten für die Lizenzierung der OIG-Funktionalität und den Standardsupport für eine Anwenderbasis mit 5.000 Identitäten.
- **Implementierungs- und Bereitstellungsaufwand in Höhe von 28.000 USD.** Dieser Betrag umfasst die einmalige Einrichtung, das interne Projektmanagement und den Konfigurationsaufwand sowie die einfacheren fortlaufenden Arbeiten zur Wartung und Pflege von Governance-Abläufen und Richtlinien.

Die Finanzanalyse auf Basis der Befragungen ergab, dass das Modellunternehmen über einen Zeitraum von drei Jahren einen Nutzen von 2,6 Mio. USD gegenüber Kosten von 849.000 USD erzielt. Daraus ergeben sich ein Kapitalwert von 1,8 Mio. USD und ein ROI von 211 %.

Gesamte Arbeitsersparnisse und Effizienzgewinne bei der Identity Governance, bei Audits und Compliance-Aufgaben sowie durch Verbesserungen der Zugriffs-Governance

1,8 Mio. $

„[OIG] erfüllt vom ersten Tag an alles, was es soll – und noch mehr. Man bekommt genau die Funktionen, die man für die Compliance braucht, und die Anwender sind zufrieden. Das sagt für mich alles."

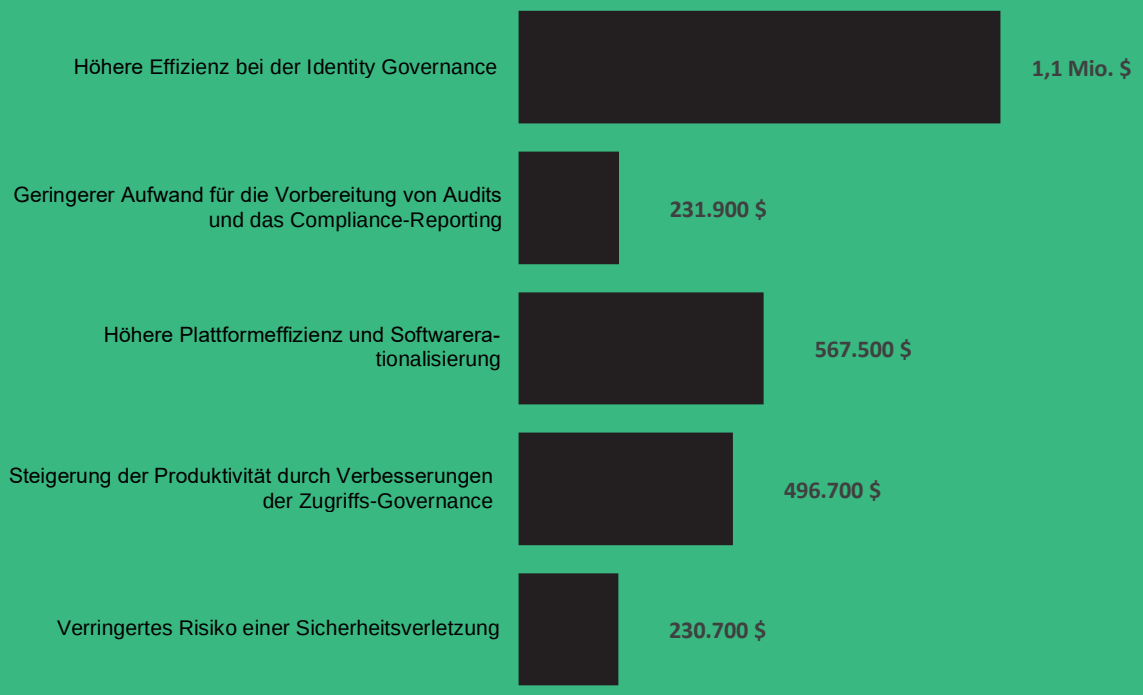
SENIOR DIRECTOR, GLOBALER IAM-LEITER, FACHDIENSTLEISTUNGEN

„Wenn wir uns die Arbeitsersparnisse bei allen Anwendern ansehen – ob Service Desk, Sicherheit, Audit, Anwendungsverantwortliche und die Führungskräfte, die Zugriffsanforderungen überprüfen und genehmigen müssen –, dann rechtfertigen diese Arbeitsersparnisse die Gesamtkosten. Dass wir das Risiko im Unternehmen verringern und unser Sicherheitsniveau erhöhen konnten, ist ebenfalls ein großer Vorteil."

CIO, FINANZDIENSTLEISTUNGEN

KAPITALRENDITE	NUTZEN (BW)	KAPITALWERT	AMORTISATION
211 %	**2,6 Mio. $**	**1,8 Mio. $**	**< 6 Monate**

Nutzen (über drei Jahre)



TEI – FRAMEWORK UND METHODIK

Aus den in den Befragungen erfassten Daten hat Forrester eine Rahmenstruktur zum Total Economic Impact™ für Unternehmen erstellt, die eine Investition in Identity Governance in Erwägung ziehen.

Mithilfe dieses Modells lassen sich Kosten, Nutzen, Flexibilität und Risikofaktoren ermitteln, die für diese Investitionsentscheidung von Bedeutung sind. Forrester verfolgte einen mehrstufigen Ansatz, um die möglichen Auswirkungen von Identity Governance in einem Unternehmen zu bewerten.

HINWEISE

Wir bitten unsere Leser um Beachtung der folgenden Punkte:

Diese Studie wurde von Okta in Auftrag gegeben und von Forrester Consulting durchgeführt. Sie ist nicht als Wettbewerbsanalyse zu verstehen.

Forrester trifft hierin keinerlei Annahmen über die potenzielle Kapitalrendite, die andere Unternehmen erzielen werden. Forrester empfiehlt den Lesern dringend, mithilfe der in der Studie dargelegten Rahmenstruktur eigene Prognosen zu erstellen, um die Angemessenheit einer Investition in Identity Governance zu ermitteln.

Zwar hat Okta Überprüfungen vorgenommen und Forrester Rückmeldung gegeben, doch behält sich Forrester die redaktionelle Kontrolle über die Studie und ihre Ergebnisse vor und genehmigt keine Änderungen an der Studie, die den Erkenntnissen von Forrester widersprechen oder die Bedeutung der Studie verfälschen würden.

Okta hat die Kundennamen für die Befragungen bereitgestellt, an den Befragungen jedoch nicht teilgenommen.

1. **Due Diligence**
   Es wurden Okta-Vertreter und Forrester-Analysten befragt, um Daten zu Identity Governance zu erheben.
2. **Befragungen**
   Um Daten zu Kosten, Nutzen und Risiken zu erhalten, wurden acht Vertreter aus Unternehmen befragt, die Identity Governance bereits einsetzen.
3. **Modellunternehmen**
   Auf Grundlage der Merkmale der befragten Unternehmen wurde ein Modellunternehmen konzipiert.
4. **Finanzmodell**
   Unter Anwendung der Methodik des TEI wurde ein Finanzmodell erstellt, das die Aussagen der Interviewpartner widerspiegelt. Dieses Modell wurde risikobereinigt und gemäß den geäußerten Problemen und Bedenken der Befragten risikoangepasst.
5. **Fallstudie**
   Vier fundamentale Elemente der Methodik des TEI bilden die Grundlage für die Modellierung der Investitionseffekte: Nutzen, Kosten, Flexibilität und Risiken. Dank immer ausgefeilterer ROI-Analysen im Zusammenhang mit IT-Investitionen bietet die Methodik des TEI von Forrester ein umfassendes Bild der gesamten wirtschaftlichen Auswirkungen von Investitionsentscheidungen. Weitere Informationen zur Methodik des TEI finden Sie in Anhang A.

Die Customer Journey von Okta Identity Governance

Beweggründe für die Investition in Identity Governance

Befragungen			
Funktion	**Branche**	**Region**	**Identitäten/verwaltete Apps**
Geschäftsführer, IAM	IT-Dienstleistungen	Globale Niederlassungen mit Hauptsitz in Nordamerika	104.000/200
Leiter der Sicherheitsarchitektur	IT-Beratung	Globale Niederlassungen mit Hauptsitz in Nordamerika	100.000/1.500
Geschäftsführer	Finanzdienstleistungen	Globale Niederlassungen mit Hauptsitz in Nordamerika	70.000/90
Senior Director, globaler IAM-Leiter	Fachdienstleistungen	Globale Niederlassungen mit Hauptsitz in Nordamerika	8.000/400
CIO	Finanzdienstleistungen	Weltweit, Unternehmenssitz in der EMEA-Region	8.000/100
Leiter der Informationssicherheit	Gesundheitswesen	Nordamerika	7.200/370
IT-Lösungsarchitekt	Softwarebranche	Globale Niederlassungen mit Hauptsitz in Nordamerika	3.000/70
CISO	IT-Dienstleistungen	EMEA	2.200/200

ZENTRALE HERAUSFORDERUNGEN

Vor der Bereitstellung von Okta Identity Governance waren den Angaben der Befragten zufolge durch die Kombination aus veralteten IGA-Plattformen, selbstentwickelten Tools und manuellen Arbeitsabläufen fragmentierte Identitätsumgebungen entstanden. Diese Umgebungen zogen nicht nur ineffiziente Betriebsabläufe für IT-Teams nach sich, sondern auch Lücken bei der Compliance und Zugriffskontrolle für Sicherheitsteams. Zugriffsanforderungen erfolgten oft über ein Ticketsystem, Zertifizierungen wurden mit Tabellenkalkulationen gesteuert und die Berechtigungsverwaltung war nicht standardisiert. Diese Einschränkungen führten zu inkonsistenten Anwendererlebnissen und erhöhten das Compliance-Risiko. Zusätzlich stellten sie eine übermäßige Belastung für die IT- und Sicherheitsteams dar.

Die Befragten nannten mehrere typische Herausforderungen, unter anderem:

- **Manuelle Bereitstellung und Zugriffsänderungen und damit eine verzögerte Produktivität und Risiken.** Viele Befragte gaben an, dass Zugriffsrechte über den Helpdesk-Tickets vergeben und entzogen wurden und dass die Dienstleistungsvereinbarung für die Bearbeitung fünf Tage oder mehr zugestand. Anderen Befragten zufolge hatten Anwender noch lange nach dem Offboarding oder Rollenwechsel Zugriffsrechte, die ihnen nicht mehr zustanden, was das Risiko der schleichenden Ausbreitung von Zugriffsrechten und internen Bedrohungen erhöhte. Laut dem IT-Lösungsarchitekt aus der Softwarebranche wurde sein Team von Zugriffsanforderungen überflutet und benötigte zusätzliches Personal, um diese Arbeitslast zu bewältigen. „Wir hatten gut 30 Personen. Die Arbeit wurde gleichmäßig auf alle verteilt. Da mein kleines Team aus drei IAM-Experten nicht in der Lage gewesen wäre, alle Zugriffsanforderungen zu bearbeiten, wurde daraus ein Gemeinschaftsprojekt."
- **Lange, arbeitsaufwendige und fehleranfällige Zugriffszertifizierungen.** Die Unternehmen stützten sich stark auf Tabellenkalkulationen und manuelle Bescheinigungen, um Audit- und Compliance-Anforderungen zu erfüllen. Mehrere Befragte berichteten, dass Zertifizierungen oft eine mehrwöchige Vorbereitung durch IAM-Mitarbeiter erfordert und einen mehrstündigen Überprüfungsaufwand für Vorgesetzte und Geschäftsinhaber nach sich gezogen haben. Der Leiter der Informationssicherheit aus dem Gesundheitswesen beschrieb Kampagnen als „Zumutung" und sagte: „Wir haben unsere Zertifizierungen im Endeffekt nie abgeschlossen. Sie scheiterten noch während der Kampagne, weil wir so viel Ablehnung von Führungskräften erfuhren. Da sie sich weigerten, die Zertifizierung vorzunehmen, kamen wir nie an den Punkt, an dem wir sagen konnten, dass wir unsere Richtlinie wirklich einhalten."
- **Eine Berechtigungsverwaltung, der es an Transparenz und Standardisierung mangelte.** Ohne zentrale Governance wurde der rollenbasierte Zugriff nicht einheitlich angewendet. Aus diesem Grund besaßen Anwender oft übermäßig viele oder veraltete Berechtigungen. Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister erklärte, dass „die Anwender Zugriffsberechtigungen gerne horten" – und dass sein Team Konten, die zu viele Berechtigungen aufwiesen, manuell identifizieren und bereinigen musste.
- **Eine Auditvorbereitung mit einem hohen Zeit- und Koordinierungsbedarf.** Die Befragten beschrieben Audits vor dem Einsatz von OIG als äußerst arbeitsaufwendig. Sie bedurften häufig einer mehrwöchigen Vorbereitung und der Arbeit von mehreren Personen, um Zugriffsprotokolle zusammenzustellen, den Abschluss von Überprüfungen zu verfolgen und auf die Auditergebnisse zu reagieren.

> „[Vor OIG] fürchteten alle unseren Besuch, aber heute werden wir als Treiber fürs Geschäft wahrgenommen. Das ist ganz schön klasse.“
>
> IT-LÖSUNGSARCHITEKT, SOFTWAREBRANCHE

> „Wir konnten zahlreiche manuelle Aufgaben eliminieren, die fehleranfällig waren, und unsere Präzision bei der Kontobereitstellung und -verwaltung [mit OIG] erhöhen, ob für Anwendungen, Anwender oder Kunden.“
>
> CIO, FINANZDIENSTLEISTUNGEN

MODELLUNTERNEHMEN

Auf der Grundlage der durchgeführten Befragungen erstellte Forrester zur Veranschaulichung der finanziellen Auswirkungen einen TEI-Bezugsrahmen, ein Modellunternehmen und eine ROI-Analyse. Das Modellunternehmen steht repräsentativ für die Unternehmen der Befragungsteilnehmer. Die aggregierte Finanzanalyse im nächsten Abschnitt basiert auf diesem Modellunternehmen. Das Modellunternehmen weist die nachfolgenden Eigenschaften auf:

Beschreibung des Modellunternehmens. Das globale Unternehmen verzeichnet einen Jahresumsatz in Höhe von 1,5 Mrd. USD und verfügt über 5.000 Identitäten und 100 Anwendungen. Das IAM-Team umfasst 10 VZÄ, die sich um das Identity Engineering, die Governance-Abläufe, die Richtliniendurchsetzung und um Zertifizierungskampagnen kümmern, sowie zwei VZÄ zur Audit- und Compliance-Unterstützung. Vor der Implementierung von OIG nutzte das Unternehmen Okta für Identitätsservices, neben einer separaten alten Lösung und manuellen Prozessen für die Zugriffs-Governance.

Merkmale der Bereitstellung. Das Modellunternehmen stellt OIG-Komponenten für Zugriffszertifizierungen und -anforderungen, die Verwaltung von Berechtigungen, Audits und das Compliance-Reporting und die Automatisierung mit Okta Workflows in einer achtwöchigen Implementierungsphase zu Beginn des ersten Jahres bereit.

GRUNDLEGENDE ANNAHMEN

1,5 Mrd. USD Umsatz

5.000 Identitäten

Ein IAM-Team mit 10 VZÄ für die Verwaltung der Identity Governance und zwei VZÄ für die Audit- und Compliance-Unterstützung

Nutzenanalyse

Daten zum quantifizierten Nutzen, angewendet auf das Modellunternehmen

Gesamtnutzen						
Ref.	**Nutzen**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Atr	Höhere Effizienz bei der Identity Governance	323.366 $	475.538 $	570.645 $	1.369.548 $	1.115.709 $
Btr	Geringerer Aufwand für die Vorbereitung von Audits und das Compliance-Reporting	69.401 $	99.144 $	115.668 $	284.213 $	231.932 $
Ctr	Höhere Plattformeffizienz und Softwarerationalisierung	225.900 $	229.500 $	229.500 $	684.900 $	567.460 $
Dtr	Steigerung der Produktivität durch Verbesserungen der Zugriffs-Governance	199.750 $	199.750 $	199.750 $	599.250 $	496.749 $
Etr	Verringertes Risiko einer Sicherheitsverletzung	92.757 $	92.757 $	92.757 $	278.270 $	230.672 $
	Gesamtnutzen (risikobereinigt)	911.173 $	1.096.688 $	1.208.320 $	3.216.181 $	2.642.522 $

HÖHERE EFFIZIENZ BEI DER IDENTITY GOVERNANCE

Fakten und Daten. Nach Angaben der Befragten gab es in ihren Unternehmen vor der Bereitstellung von Okta Identity Governance umfangreiche manuelle Prozesse für Zugriffszertifizierungen, für die Berechtigungsverwaltung und die Bearbeitung von Ad-hoc-Zugriffsanforderungen.

- Der IAM-Leiter bei einem IT-Dienstleister berichtete über den Schwerpunkt, den sein Team auf Automatisierung und Self-Service-Funktionen legt: „Das Volumen [von IAM-Aufgaben], das mehr als 36 Vollzeitangestellte beschäftigte, die alle dieselben Arbeiten durchführten, kann nun im Wesentlichen von fünf [Mitarbeitern mit OIG] bewältigt werden. Dank der Funktionen von OIG und der Automatisierung mit Workflows benötigen wir dafür keine zusätzlichen Lösungen. Wir arbeiten innerhalb der Okta-Plattform und nutzen die Low-Code- und No-Code-Workflows für Automatisierungen.“

- Der IAM-Leiter fügte hinzu, dass sein Unternehmen pro Monat zwischen 80 und 90 Kampagnen mit 20.000 bis 80.000 Aktionen durchführe, die das IAM-Team in jeweils unter einer Stunde ausführen könne.
- Der Leiter der Informationssicherheit bei einem Unternehmen aus dem Gesundheitswesen sagte: „In der Informationssicherheit brauchten ein Engineer und ein Analyst ungefähr vier Wochen, um eine Kampagne vorzubereiten. Sie mussten jeden einzelnen Schritt überwachen und Vorgesetzte durchgängig anleiten – manchmal mehrere hundert gleichzeitig. Zwei Ressourcen waren quasi ein Viertel des Jahres nur damit beschäftigt, Zugriffsüberprüfungen durchzuführen. Jetzt dauert die Einrichtung 30 Minuten."
- Der CIO des Finanzdienstleisters sagte: „[Mit OIG] konnten wir den Automatisierungsgrad von 50 % auf 90 % erhöhen und den Arbeitsaufwand um die Hälfte verringern."
- Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister schätzt, dass sein IAM-Team, das neun Mitglieder umfasst, nun die Arbeit von 14 bis 15 Personen erledigt.
- Der CISO eines IT-Dienstleisters nannte die von OIG ermöglichte Automatisierung einen Spitzenvorteil und erklärte, dass sein Unternehmen „im Grunde alles auf Workflows und automatisierte Prozessen basiert, um den manuellen Aufwand zu beseitigen".
- Der IT-Lösungsarchitekt eines Softwareunternehmens sprach die Auswirkungen von Okta Workflows an: „Automatisierung gab es bei uns zwar schon, aber die war ein ziemliches Sammelsurium: PowerShell-Skripte, Python-Skripte, AWS-Lambda-Funktionen, ein einziges Durcheinander. Wir konnten dies alles in den Okta Workflow-Stack migrieren und dann die integrierten Hooks in all unseren unterschiedlichen Identitätsabläufen einsetzen. Damit haben wir die Komplexität drastisch verringert – und den Zeitaufwand für die Wartung dieser Plattformen gleich mit."

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- Zehn IAM-VZÄ sind für die wichtigen Aufgaben der Identity Governance zuständig, u. a. für Zugriffsanforderungen und -überprüfungen und die Berechtigungsverwaltung.
- Das durchschnittliche Jahresgehalt (inkl. Nebenkosten) für ein IAM-VZÄ beläuft sich auf 140.900 USD.
- Nach der achtwöchigen Implementierungsphase spart das Team in den verbleibenden 44 Wochen 40 % der Zeit ein, die auf die Identity Governance entfällt. Damit ergeben sich im ersten Jahr Nettoeinsparungen in Höhe von 34 %.

- Diese Zeiteinsparungen steigen im zweiten Jahr auf 50 % und im dritten auf 60 %, da mehr Anwendungen durch OIG verwaltet und mehr Automatisierungen integriert werden und der manuellen Aufwand damit noch weiter sinkt.
- Die gewonnene Zeit wird zu 75 % für andere Tätigkeiten mit Mehrwert genutzt.

Risiken. Zur Untermauerung realistischer und fundierter Schätzungen passt Forrester die Risikowerte an – abhängig von der Übereinstimmung der Interviewdaten und der Streuung der gemeldeten Resultate. Mit dieser Komponente der TEI-Methodik werden Unterschiede zwischen Implementierungsumgebungen berücksichtigt. Der Betrag dieses Nutzens kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- dem Automatisierungsgrad und den Zeiteinsparungen, die je nach Komplexität der alten Systeme oder Compliance-Anforderungen variieren
- dem Bedarf an manueller Beaufsichtigung, der in Unternehmen mit regulatorischen oder branchenspezifischen Einschränkungen höher ausfallen kann
- dem Umfang des Nutzens, der vom Anwendervolumen, der Kampagnenhäufigkeit und der Anzahl und Komplexität der verwalteten Anwendungen abhängt
- dem durchschnittlichen Jahresgehalt (inkl. Nebenkosten) für ein IAM-VZÄ

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 % nach unten korrigiert. So ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 1,1 Mio. USD.

Eingesparte Zeit für Aufgaben der Identity Governance im 3. Jahr

60 %

„Wir können jetzt problemlos zehnmal so viel erledigen wie mit [der alten Lösung] – vielleicht sogar mehr.“

LEITER INFORMATIONSSICHERHEIT, GESUNDHEITSWESEN

„Workflows sparen viele VZÄ ein. Angesichts der Anzahl an Anwendungen, die wir besitzen, könnten wir den Aufwand anders gar nicht bewältigen.“

LEITER SICHERHEITSARCHITEKTUR, IT-BERATUNG

Höhere Effizienz bei der Identity Governance					
Ref.	**Kennzahl**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
A1	IAM-VZÄ werden Zugriffsanforderungen und -überprüfungen, der Verwaltung von Berechtigungen und anderen Aufgaben der Identity Governance zugeteilt.	Modellunternehmen	10	10	10
A2	Jahresgehalt (inkl. Nebenkosten) für ein IAM-VZÄ mit Aufgaben der Identity Governance	Modellunternehmen	140.900 $	140.900 $	140.900 $
A3	Netto-Zeiteinsparung nach der Implementierung von OIG für Aufgaben der Identity Governance	Befragungen	34 %	50 %	60 %
A4	Produktivitätsrückgewinnung	Methodik des TEI	75 %	75 %	75 %
At	Höhere Effizienz bei der Identity Governance	A1*A2*A3*A4	359.295,0 $	528.375,0 $	634.050,0 $
	Risikobereinigung	↓ 10 %			
Atr	Höhere Effizienz bei der Identity Governance (risikobereinigt)		323.365,50 $	475.537,50 $	570.645,00 $
	Gesamtwert über drei Jahre: 1.369.548 $		**Barwert über drei Jahre: 1.115.709 $**		

GERINGERER AUFWAND FÜR DIE VORBEREITUNG VON AUDITS UND DAS COMPLIANCE-REPORTING

Fakten und Daten. Die Befragten können nach eigener Aussage mit OIG den großen manuellen Aufwand für regelmäßig anstehende Audits, Zugriffsüberprüfungen und das Compliance-Reporting optimieren oder vermeiden. Teams, die zuvor dafür verantwortlich waren, Zugriffskontrollen zu validieren und Bescheinigungen und Berichte vorzubereiten, meldeten deutliche

Zeiteinsparungen und einen geringeren Arbeitsaufwand im Zusammenhang mit Audits. Zu den konkreten Bereichen, in denen der Aufwand reduziert oder beseitigt wurde, gehörten die folgenden:

- Die Befragten berichteten, dass vor der Einführung von OIG Audits einer wochenlangen Vorbereitung bedurften. Diese Arbeiten umfassten die manuelle Zusammenstellung der Zertifizierungsdaten, die Erstellung von Screenshots von Zugriffsgenehmigungen und die systemübergreifende Validierung von Protokollen der Zugriffskontrolle.
- Mehrere Befragte gaben an, dass die Automatisierung der Zertifizierungsabläufe die Vollständigkeit und Konsistenz der Überprüfungsprozesse verbessert habe. Es gebe weniger fehlende oder falsche Datensätze, die negative Audit-Ergebnisse mit sich bringen können. Außerdem nannten die Befragten zentralisierte Richtlinien, Arbeitsabläufe und Auditprotokolle in OIG als Faktoren, aufgrund derer die Erklärung von Governance-Prozessen gegenüber Prüfern und Dokumentenausnahmen nun weniger mühsam sei.
- Die Befragten gaben an, dass sie Zeit einsparen und die Komplexität verringern konnten, indem sie mit OIG-Dashboards Ad-hoc-Berichte zu Zugriffsüberprüfungen, Benutzerrollen und Berechtigungen erzeugen. Dank dieser Funktionen können die Teams schneller auf interne Audit- oder externe regulatorische Anfragen reagieren.
- Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister erläuterte, dass er ohne die Automatisierung mit OIG zur Sammlung von Nachweisen „ein drei- bis fünfköpfiges Team benötigt hätte, um für Einheitlichkeit zu sorgen“.
- Er fügte hinzu: „Ich kann einem Prüfer jetzt in nur 30 Minuten alle nötigen Daten vorlegen – und damit ist das Ganze erledigt. Es kommen keine Nachfragen. [Der Prüfer] wandte sich nur [im Auftrag seines] Sicherheits-Engineers erneut an mich, damit man bei ihnen auch [OIG] implementieren konnte. Das ist zweimal passiert. Das ist das größte Kompliment aller Zeiten.“

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- Audit- und Compliance-Aufgaben werden zwei VZÄ zugeteilt.
- Das durchschnittliche Jahresgehalt (inkl. Nebenkosten) für ein Audit- und Compliance-VZÄ beläuft sich auf 122.400 USD.
- Nach der achtwöchigen Implementierungsphase spart das Team in den verbleibenden 44 Wochen 50 % der Zeit ein, die auf die Auditvorbereitung und das Compliance-Reporting entfällt. Damit ergeben sich im ersten Jahr Nettoeinsparungen in Höhe von 42 %.

- Diese Zeiteinsparungen erhöhen sich im zweiten Jahr auf 60 % und im dritten auf 70 %, da das IAM-Team effizienter arbeitet und die OIG-Governance ausgeweitet wird.
- Diese Zeitersparnisse werden zu 75 % auf andere wertschöpfende Tätigkeiten umverteilt.

Risiken. Der Betrag dieses Nutzens kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- der Anzahl und Komplexität der erforderlichen Audits, basierend auf der Branche und der Region
- der Reife der Prozesse und Tools, die vor der Einführung von OIG vorhanden waren
- der Größe und Struktur der IAM- und Compliance-Teams
- dem Grad der Automatisierung Audit-bezogener Aufgaben und ihrer in andere Governance-Systeme
- dem durchschnittlichen Jahresgehalt (inkl. Nebenkosten) für ein Audit- und Compliance-VZÄ

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen 10 % niedriger angesetzt. So ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 232.000 USD.

Zeiteinsparungen bei Audit- und Compliance-Aufgaben im dritten Jahr
70 %

Geringerer Aufwand für die Vorbereitung von Audits und für das Compliance-Reporting					
Ref.	**Kennzahl**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
B1	IAM-VZÄ mit Audit- und Compliance-Aufgaben	Modellunternehmen	2	2	2
B2	Jahresgehalt (inkl. Nebenkosten) für ein IAM-VZÄ mit Audit- und Compliance-Aufgaben	Modellunternehmen	122.400 $	122.400 $	122.400 $
B3	Netto-Zeiteinsparungen bei Audit- und Compliance-Aufgaben mit OIG	Befragungen	42 %	60 %	70 %
B4	Produktivitätsrückgewinnung	Methodik des TEI	75 %	75 %	75 %
Bt	Geringerer Aufwand für die Vorbereitung von Audits und für das Compliance-Reporting	B1*B2*B3*B4	77.112,00 $	110.160,00 $	128.520,00 $
	Risikobereinigung	↓ 10 %			
Btr	Geringerer Aufwand für die Vorbereitung von Audits und für das Compliance-Reporting (risikobereinigt)		69.400,80 $	99.144,00 $	115.668,00 $
	Gesamtwert über drei Jahre: 284.213 $		**Barwert über drei Jahre: 231.932 $**		

HÖHERE PLATTFORMEFFIZIENZ UND SOFTWARERATIONALISIERUNG

Fakten und Daten. Wie die Befragten berichteten, gelang ihnen mit Okta Identity Governance eine Steigerung der Plattformeffizienz, da die Abhängigkeit von kostspieligen externen Beratern verringert, benutzerdefinierte Konnektoren beseitigt und interne Teams mit Low-Code- bzw. No-Code-Tools ausgestattet wurden. Gleichzeitig erhielten die Unternehmen eine höhere Transparenz hinsichtlich der Berechtigungen und bessere Einblicke in die Nutzung. So konnten sie die Software-Ausgaben straffen und ungenutzte Lizenzen entfernen. All diese Änderungen erhöhten die betriebliche Effizienz und stärkten die Governance-Abdeckung.

Plattformeffizienz:

- Der Leiter der Informationssicherheit aus dem Gesundheitswesen berichtete, dass sein Unternehmen vor der Einführung von OIG pro Jahr zwischen 150.000 und 200.000 USD für Berater ausgegeben habe, um Projekte mit veralteten Lösungen voranzubringen. Mit OIG entfallen diese zusätzlichen Kosten – dank der vorkonfigurierten Konnektoren, der Low-Code- und No-Code-Automatisierung und der Unterstützung der internen Teams durch modernere Tools.
- Der CIO des Finanzdienstleisters fügte hinzu: „[OIG] umfasst viele vorgefertigte Integrationen. Das hat es uns leicht gemacht, OIG mit unserer aktuellen Umgebung zu

verbinden. [OIG] verschafft uns außerdem Vorteile bei der Lizenz- und Ressourcenverwaltung, da wir nun weniger ungenutzte Konten behalten.“

- Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister habe 15.000 bis 25.000 USD für die Vernetzung von Anwendungen gezahlt, mit dem folgenden Ergebnis: „Man vernetzt nicht alle Systeme, die man für die Governance vernetzen würde. Es besteht also das Risiko, dass es hier Lücken gibt, weil manche Systeme nicht über eine API verbunden sind. [Mit OIG] wurde jedes System, das eine SSO-Verbindung mit meinem Identitätsanbieter aufwies, automatisch zur Governance hinzufügt. Und so sollte es auch sein.“

Softwarerationalisierung:

- Wie die Befragten erklärten, half ihnen die Berechtigungstransparenz von OIG, ungenutzte und doppelt vorhandene Lizenzen zu identifizieren und zu entfernen. Das Softwareunternehmen des IT-Lösungsarchitekt führt seinen Angaben nach Ad-hoc-Zertifizierungskampagnen durch, um in Echtzeit zu erkennen, von wem Anwendungen tatsächlich verwendet werden, und „zieht daraus stets großen Nutzen“. In einem Fall konnten etwa 200 Lizenzen für eine Anwendung mit 550 Anwendern zu einem Preis von 5–10 USD pro Anwender und Monat abgeschafft werden.
- Auf die Frage, welche Einsparungen durch die Erhöhung der Plattformeffizienz und die Softwarerationalisierung möglich waren, nannte der CIO eines Finanzdienstleisters einen Betrag von mehr als 200.000 USD pro Jahr.

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- Das Unternehmen verbindet 10 inkrementelle Anwendungen mit OIG, wofür bei der alten Lösung ein kostenpflichtiger Konnektor vonnöten gewesen wäre.
- Die Konnektorgebühren betragen 20.000 USD je Anwendung.
- OIG ermöglicht die Lizenzbereinigung für 10 Anwendungen, mit durchschnittlich 50 entfernten ungenutzten oder doppelt vorhandenen Lizenzen und monatlichen Kosten in Höhe von 5 USD pro Lizenz.
- Nach der achtwöchigen Implementierungsphase spart das Unternehmen im ersten Jahr 21.000 USD und im zweiten und im dritten Jahr 25.000 USD bei den Kosten für Berater bzw. externen Support.

Risiken. Der Betrag dieses Nutzens kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- den Kosten und der Verfügbarkeit von vorgefertigten Konnektoren für alte IGA-Lösungen
- der Anzahl und den Arten der Anwendungen, die über OIG hinzugefügt bzw. verwaltet werden
- den Lizenzstrukturen und den Mustern der übermäßigen Bereitstellung in den Softwareumgebungen des Unternehmens
- der Abhängigkeit von externen Beratern bzw. Managed-Service-Anbietern für IAM-Funktionen

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 % nach unten korrigiert. So ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 568.000 USD.

Höhere Plattformeffizienz und Softwarerationalisierung					
Ref.	**Kennzahl**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
C1	Konnektorgebühren pro Anwendung bei der alten Lösung	Befragungen	20.000 $	20.000 $	20.000 $
C2	Inkrementelle Anwendungsverbindungen dank OIG	Modellunternehmen	10	10	10
C3	**Zwischensumme: mit OIG eingesparte Konnektorgebühren**	**C1*C2**	**200.000 $**	**200.000 $**	**200.000 $**
C4	Anwendungen mit Lizenzbereinigung mit OIG	Modellunternehmen	10	10	10
C5	Pro Anwendung entfernte nicht benötigte Lizenzen	Befragungen	50	50	50
C6	Durchschnittliche Lizenzkosten pro Anwender und Monat	Befragungen	5 $	5 $	5 $
C7	**Zwischensumme: mit OIG eingesparte Lizenzgebühren**	**C4*C5*C6*12**	**30.000 $**	**30.000 $**	**30.000 $**
C8	Eingesparte Kosten für Beratung bzw. externen Support für IAM	Befragungen	21.000 $	25.000 $	25.000 $
Ct	Höhere Plattformeffizienz und Softwarerationalisierung	C3+C7+C8	251.000,00 $	255.000,00 $	255.000,00 $
	Risikobereinigung	↓ 10 %			
Ctr	Höhere Plattformeffizienz und Softwarerationalisierung (risikobereinigt)		225.900 $	229.500 $	229.500 $
	Gesamtwert über drei Jahre: 684.900 $		**Barwert über drei Jahre: 567.460 $**		

STEIGERUNG DER PRODUKTIVITÄT DURCH VERBESSERUNG DER ZUGRIFFS-GOVERNANCE

Fakten und Daten. Die Befragten beschrieben, wie sie mit OIG die zugriffsbezogenen Arbeitsabläufe für Endanwender, Vorgesetzte und Anwendungsverantwortliche optimiert haben. Vor der Einführung von OIG kam es häufig zu übermäßigen Anforderungen und damit zu Verzögerungen und gesonderten Nachfragen. Da mit OIG die Anforderungen effizienter weitergeleitet und bearbeitet werden, werden die anfordernden Personen und Genehmiger entlastet. Durch die Automatisierung und Vereinfachung von Zugriffsanforderungen, Zertifizierungen und Berechtigungsüberprüfungen konnte der Zeitaufwand für die Navigation in veralteten Benutzeroberflächen, das Warten auf manuelle Genehmigungen und die Reaktion auf inkonsistente Governance-Prozesse verringert werden.

- Dazu der IT-Lösungsarchitekt aus der Softwarebranche: „[Ohne OIG] dauerte der Abschluss von Genehmigungen 45 Minuten bis zwei Stunden und wir mussten bis zu 24 Stunden warten, bis der Zugriff gewährt wurde. Wir konnten die Zeit für die vollständige Bearbeitung der Anforderung auf 30 Minuten verkürzen.“
- Der Geschäftsführer des Finanzdienstleisters berichtete im Hinblick auf Zugriffsanforderungen oder Veränderungen: „Sonst haben wir fünf Werktage dafür gebraucht, jetzt wurde der Vorgang automatisiert und ist nach 30 Minuten abgeschlossen.“

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- 5.000 Endanwender sparen mit OIG durchschnittlich 2 Stunden pro Jahr, da weniger Zugriffsprobleme auftreten und die Zugriffsgenehmigung und -bereitstellung optimiert ist.
- Der durchschnittliche Stundensatz (inkl. Nebenkosten) eines Endanwenders beträgt 47 USD.

Risiken. Der Betrag dieses Nutzens kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- den Arten und dem Volumen der zugriffsbezogenen Aufgaben, die Unternehmensanwendern zugewiesen werden
- der Reife und Konsistenz der Governance-Abläufe vor der Implementierung von OIG
- dem Grad der Automatisierung und Anpassung, die beim Rollout bereitgestellt wurde

- dem Verbreitungsgrad der Anforderungs- und Zertifizierungsabläufe im gesamten Unternehmen
- dem durchschnittlichen Stundensatz (inkl. Nebenkosten) eines Endanwenders

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 15 % nach unten korrigiert. Daraus ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 497.000 USD.

Wert der Zeiteinsparungen für Endanwender durch Verbesserungen der Zugriffs-Governance

497.000 $

„[OIG] hat das Anwendererlebnis drastisch verbessert. Die Anwender können ihre Aufgaben nun sehr schnell erledigen und sich wieder ihrer eigentlichen Arbeit zuwenden, wohingegen sie in der Vergangenheit deutlich an Produktivität verloren haben."

GESCHÄFTSFÜHRER, FINANZDIENSTLEISTUNGEN

Steigerung der Produktivität durch Verbesserungen der Zugriffs-Governance

Ref.	Kennzahl	Quelle	Jahr 1	Jahr 2	Jahr 3
D1	Endanwender gesamt	Modellunternehmen	5.000	5.000	5.000
D2	Durchschnittlich eingesparte Stunden pro Endanwender dank optimierter Zugriffsgenehmigung und -bereitstellung und weniger Zugriffsproblemen mit OIG	Befragungen	2	2	2
D3	Stundensatz (inkl. Nebenkosten) für einen Endanwender	Modellunternehmen	47 $	47 $	47 $

D4	Produktivitätsrückgewinnung	Methodik des TEI	50 %	50 %	50 %
Dt	Steigerung der Produktivität durch Verbesserungen der Zugriffs-Governance	D1*D2*D3*D4	235.000 $	235.000 $	235.000 $
	Risikobereinigung	↓ 15 %			
Dtr	Steigerung der Produktivität durch Verbesserung der Zugriffs-Governance (risikobereinigt)		199.750 $	199.750 $	199.750 $
	Gesamtwert über drei Jahre: 599.250 $		**Barwert über drei Jahre: 496.749 $**		

VERRINGERTES RISIKO EINER SICHERHEITSVERLETZUNG

Fakten und Daten. Die Befragten bestätigten, dass es ihnen mit Okta Identity Governance gelungen ist, das Risiko von Sicherheitsverletzungen zu reduzieren. Möglich wurde dies durch die Durchsetzung des Zugriffs nach dem Least-Privilege-Prinzips, den Entzug unnötiger Berechtigungen und die Automatisierung von Überprüfungen und Löschungen. Einige Befragten betonten, dass OIG dazu beigetragen habe, die schleichende Ausbreitung von Zugriffsrechten einzudämmen und veraltete Zugriffsberechtigungen zu bereinigen – in den Augen der Studienteilnehmer eine entscheidende Fähigkeit, um eine Zero-Trust-Architektur zu realisieren.

- Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister sagte, dass OIG seinem Unternehmen geholfen habe, übermäßig bereitgestellte Zugriffsrechte zu reduzieren und menschliche Fehler zu minimieren - Probleme, die das Unternehmen in der Vergangenheit unnötigen Risiken ausgesetzt hatten. „Unsere Mitarbeiter mögen diese Trennung von Pflichten und toxischen Berechtigungen. Mit der Automatisierung [von OIG] werden die Rollen, die man aktuell besitzt, schnell überprüft. So wird sichergestellt, dass die angeforderte Rolle keine toxische Kombination mit einer der bereits zugewiesenen Rollen bildet, und das Problem bereits im Keim erstickt. Das ist ein riesengroßer Vorteil.“
- Der Leiter der Informationssicherheit aus dem Gesundheitswesen erklärte, dass OIG eine signifikante Senkung des Risikos ermöglicht habe, das für geschützte Gesundheitsinformationen bestehe. OIG sorge für eine strengere Governance beim Zugriff auf PHI-Daten und gewährleiste damit, dass nur noch die Anwender vertrauliche Daten einsehen können, die sie für ihre Arbeit effektiv benötigen. Diese zielgerichtete Reduzierung von unnötigen Zugriffsrechten minimiere potenzielle Compliance- und Sicherheitsrisiken.

- Der CIO eines Finanzdienstleisters sagte: „Da wir Pflichten und Richtliniendurchsetzungen trennen können, sind wir in der Lage, Interessenkonflikte zu vermeiden und die Betrugsgefahr zu senken. Wir haben einen Rückgang der internen Bedrohungen verzeichnet, da wir nun eine höhere Transparenz bei diesen Zugriffsüberprüfungen und Zertifizierungen haben, insbesondere in Bezug auf Auftragnehmer und externe Partner. Die automatisierte Aufhebung der Bereitstellung stellt sicher, dass ehemaligen Mitarbeiter, Auftragnehmer und Lieferanten die Zugriffsrechte entzogen werden – das bedeutet ein geringeres Risiko für uns.“

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- Im Modellunternehmen besteht ein Risiko von Sicherheitsverletzungen von jährlich 3,027 Mio. USD.[2] Die Wahrscheinlichkeit des Auftretens mindestens einer Sicherheitsverletzung liegt bei 63 %.[3]
- Von diesen Sicherheitsverletzungen entfallen 76 % auf externe Angriffe bzw. interne Vorfälle bzw. hängen mit dem externen Ökosystem zusammen.[4]
- 80 % dieser Vorfälle lassen sich durch die bessere Identity Governance und Zugriffskontrollen von OIG verhindern.
- Basierend auf den Aussagen der Befragten senkt das Modellunternehmen durch die Implementierung von OIG seine Risikobelastung um 10 %, dank verbesserter Zugriffshygiene und effizienterer Überprüfungen.

Risiken. Der Umfang dieses Nutzens kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- der Größe, der Branche und dem inhärenten Sicherheitsrisikoprofil des Unternehmens
- der Reife und den Tools der vorhandenen Identity Governance
- der Breite der OIG-Bereitstellung und der Durchsetzung von Zugriffsrichtlinien
- der internen Abstimmung zwischen IAM-, Sicherheits- und Compliance-Teams

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 20 % niedriger angesetzt. So ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 231.000 USD.

> „Wir konnten unser Sicherheitsniveau drastisch verbessern, was unseren CISO, unsere Compliance- und Risikoteams, unsere Kunden und unsere Aktionäre zufriedenstellt. [OIG] liefert in puncto Sicherheit einen erheblichen Nutzen.“
>
> **CIO, FINANZDIENSTLEISTUNGEN**

Verringertes Risiko einer Sicherheitsverletzung					
Ref.	**Kennzahl**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
E1	Kumulative Kosten von Sicherheitsverletzungen für das Modellunternehmen	Studien von Forrester	3.027.000 $	3.027.000 $	3.027.000 $
E2	Eintrittswahrscheinlichkeit von mindestens einer Sicherheitsverletzung im Modellunternehmen	Studien von Forrester	63 %	63 %	63 %
E3	Prozentsatz der Sicherheitsverletzungen, die durch externe Angriffe auf Unternehmen oder interne Vorfällen verursacht wurden oder mit dem externen Ökosystem zusammenhängen	Studien von Forrester	76 %	76 %	76 %
E4	Prozentsatz dieser Angriffe, die mit OIG verhindert werden können	Studien von Forrester	80 %	80 %	80 %
E5	**Zwischensumme: jährliche Risikoexposition, die durch OIG gemindert werden kann**	**E1*E2*E3*E4**	**1.159.462,0 $**	**1.159.462,0 $**	**1.159.462,0 $**
E6	Kosten für das verringerte Risiko von Sicherheitsverletzungen durch Angriffe, die mit OIG gemindert werden können	Befragungen	10 %	10 %	10 %
Et	Verringertes Risiko einer Sicherheitsverletzung	E5*E6	115.946 $	115.946 $	115.946 $
	Risikobereinigung	↓20 %			
Etr	Verringertes Risiko einer Sicherheitsverletzung (risikobereinigt)		92.757 $	92.757 $	92.757 $
	Gesamtwert über drei Jahre: 278.270 $		**Barwert über drei Jahre: 230.672 $**		

NICHT QUANTIFIZIERTER NUTZEN

Die Befragten erwähnten die folgenden weiteren Vorteile für ihre Unternehmen, die sie jedoch nicht quantifizieren konnten:

- **Schnelle Time-to-Value.** Die Befragten betonten übereinstimmend, wie schnell sie OIG bereitstellen und Wert daraus generieren konnten, verglichen mit herkömmlichen IGA-Plattformen, deren Planung, Bereitstellung und Integration oft mehrere Monate in Anspruch nahm. Die Teams, die OIG nutzen, konnten die wichtigsten Fähigkeiten – darunter die Arbeitsabläufe für Zugriffsanforderungen und Zertifizierungen – mit sehr wenigen Ressourcen und minimalem Konfigurationsaufwand bereitstellen. Durch diese schnelle Einführung konnten die Unternehmen unmittelbar bedeutende Verbesserungen der Governance realisieren, sogar noch vor der vollständigen Optimierung oder dem breiten Rollout.

  Nach Angaben des CIO eines Finanzdienstleisters verkürzte OIG die Time-to-Value dank der tiefgreifenden Integration in die vorhandene Okta-Infrastruktur des Unternehmens – einschließlich Single Sign-on, Multi-Faktor-Authentifizierung und API-Zugriffsverwaltung. Da diese zentralen Services bereits vorhanden waren, konnte OIG schneller und mit weniger Integrationsschwierigkeiten bereitgestellt werden als Lösungen von Mitbewerbern.

  Der Leiter der Informationssicherheit aus dem Gesundheitswesen sagte: „Die Implementierung ging in kürzester Zeit über die Bühne. Man muss dabei eigentlich gar nichts tun. OIG ist einfach Teil der [Okta]-Plattform. Wir hatten die Lösung innerhalb von zwei Wochen im Einsatz – das war für uns ein voller Erfolg!“

  Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister berichtete von der Bereitstellung Folgendes: „Das waren damals nur zwei Engineers und ich. Wir haben an einem Donnerstag und einem Freitag telefonisch alles besprochen, und plötzlich war alles schon fertig. Wir haben Zugriffsanforderungen. Wir haben Governance und Zertifizierungen, die jetzt problemlos laufen. Setzen wir das Ganze in die Produktion. Hätten wir unseren Fähigkeiten mehr vertraut, hätten wir das schon am ersten Tag abschließen können.“

- **Bessere Arbeitsmoral im IT- und im Sicherheitsteam.** Nach Aussagen der Befragten können sich die Teams auf strategisch wichtigere Arbeiten mit größerer Wertschöpfung konzentrieren, da OIG wiederholte manuelle Aufgaben beseitigt und den

Verwaltungsaufwand für Zugriffsanforderungen und Zertifizierungen verringert hat. Dies hat sich, so die Studienteilnehmer, äußerst positiv auf die Produktivität *und* die Kultur der IT-, IAM- und Sicherheitsteams ausgewirkt. Der Leiter der Sicherheitsarchitektur bei einem IT-Beratungsunternehmen sagte: „Der manuelle Aufwand des Prozessmanagements ist jetzt geringer, sodass wir uns auf strategischere Ziele konzentrieren können." Der Senior Director und globale IAM-Leiter bei einem Fachdienstleister sagte: „Die Mitglieder meines Teams übernehmen nun quasi andere Rollen, die sie schon immer gerne innehaben wollten, für die sie aber nicht die Voraussetzungen erfüllten. Mit [OIG] kann man als Führungskraft Arbeitsaufträge anders priorisieren, weil man eine Aufgabe einer Person zuweist, die sie nicht nur als Analyst erledigen möchte, sondern wirklich den Wunsch hat, diese Aufgabe zu übernehmen. Die Teammitglieder betteln förmlich um diese Art von Aufgaben. Sie gelten als cool."

> „Die Fachkompetenz von [Okta] ist beeindruckend. Ich arbeite sehr gerne mit ihnen zusammen. Die Okta-Teams für Customer Success und Kundensupport kennen sich wirklich aus."
>
> **GESCHÄFTSFÜHRER, FINANZDIENSTLEISTUNGEN**

FLEXIBILITÄT

Flexibilität hat für jeden Kunden einen anderen Stellenwert. Es sind mehrere Szenarien denkbar, in denen ein Kunde sich für die Implementierung von Identity Governance entscheidet und später zusätzliche Anwendungs- und Geschäftsmöglichkeiten erkennt, z. B.:

- **Bessere Zukunftsfähigkeit und höhere Flexibilität.** Die Befragten nannten die Flexibilität von OIG als wichtigen Faktor sowohl für kurzfristige Gewinne als auch für langfristiges strategisches Wachstum. Mehrere Studienteilnehmer begannen ihren Berichten zufolge mit einem eng gefassten Anwendungsfall – beispielsweise Zugriffsanforderungen oder Onboarding – und weiteten diesen im Laufe der Zeit auf zusätzliche Anwendungen, Geschäftsbereiche oder Compliance-Rahmenwerke aus. Die Befragten bezeichneten diesen schrittweisen Ansatz als essenziell, um den Governance-Umfang an der internen

Bereitschaft und den sich verändernden regulatorischen Prioritäten auszurichten. Die native Integration von OIG in die Identity-Plattform von Okta ermöglichte es den Unternehmen der Befragten, ihre Lösung ohne administrativen Aufwand oder die Störung bestehender Arbeitsabläufe zu skalieren. Außerdem konnten Kontrollen für die Unterstützung verschiedener geografischer Regionen und Standards (wie SOX, HIPAA und ISO) konfiguriert werden. Der Leiter der Informationssicherheit aus dem Gesundheitswesen fasste es kurz und knapp zusammen: „[Mit OIG] hält man sein Schicksal in den eigenen Händen."

Die Flexibilität ließe sich ebenfalls quantifizieren, wenn sie im Rahmen eines konkreten Projekts bewertet würde (ausführlichere Beschreibung unter Total Economic Impact – Ansatz).

> „Das Tool, der Support, die Mechanismen, mit denen das Tool unterstützt wird – alles ist hochgradig flexibel."
>
> **SENIOR DIRECTOR, GLOBALER IAM-LEITER, FACHDIENSTLEISTUNGEN**

Kostenanalyse

Quantifizierbare Kosten, angewendet auf das Modellunternehmen

Gesamtkosten							
Ref.	**Kosten**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Dtr	OIG-Gebühren	0 $	330.000 $	330.000 $	330.000 $	990.000 $	820.661 $
Etr	Schulungen, Implementierung und Optimierung	27.878 $	0 $	0 $	0 $	27.878 $	27.878 $
	Gesamtkosten (risikobereinigt)	27.878 $	330.000 $	330.000 $	330.000 $	1.017.878 $	848.539 $

OIG-GEBÜHREN

Fakten und Daten. Die Befragten legten Kostendaten vor, die von Okta bestätigt wurden. Beim Modellunternehmen basieren die geschätzten Kosten von 5 USD pro Anwender pro Monat auf der konkreten Implementierung und dem konkreten Szenario des Modellunternehmens. Die tatsächlichen Barwertkosten variieren je nachdem, welche Services einem Kunden von Okta und OIG bereitgestellt werden. Zusätzliche Informationen erhalten Sie von Okta.

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an:

- OIG wird für 5.000 verwaltete Identitäten bereitgestellt.
- Die monatliche Gebühr beträgt 5 USD pro Identität.

Risiken. Die Kosten können bei jedem Kunden aufgrund unterschiedlicher verhandelter Preise und Lizenzstrukturen anders ausfallen.

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester die genannten Kosten um 10 % nach oben korrigiert. So ergibt sich über drei Jahre ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 821.000 USD.

OIG-Gebühren						
Ref.	**Kennzahl**	**Quelle**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**
F1	Mit OIG verwaltete Identitäten	Modellunternehmen		5.000	5.000	5.000
F2	Monatliche OIG-Gebühren pro Identität	Befragungen		5 $	5 $	5 $
Ft	OIG-Gebühren	F1*F2*12	0 $	300.000 $	300.000 $	300.000 $
	Risikobereinigung	↑ 10 %				
Ftr	OIG-Gebühren (risikobereinigt)		0 $	330.000 $	330.000 $	330.000 $
	Gesamt über drei Jahre: 990.000 $		**Barwert über drei Jahre: 820.661 $**			

SCHULUNGEN, IMPLEMENTIERUNG UND OPTIMIERUNG

Fakten und Daten. Nach Aussagen der Befragten waren für die OIG-Konfiguration, die Einarbeitung der Anwender und die Feinabstimmung der Zugriffsabläufe Schulungen sowie Implementierungs- und Optimierungsaktivitäten erforderlich. Diese Aktivitäten nahmen mehrere Wochen bis hin zu mehreren Monaten in Anspruch.

Modellierung und Annahmen. Ausgehend von den Ergebnissen der Kundenbefragungen nimmt Forrester für das Modellunternehmen Folgendes an.

- Das IAM-Team sowie die dedizierten Teams für die Audit- und Compliance-Unterstützung verbringen acht Wochen mit der Implementierung von OIG, wobei durchschnittlich 10 % der Zeit OIG-spezifischen Aufgaben zugewiesen werden.
- Der durchschnittliche Stundensatz (inkl. Nebenkosten) für ein IAM-, Audit- und Compliance-VZÄ beträgt 66 USD.

Risiken. Der Betrag dieser Kosten kann je nach Kunde variieren und hängt von folgenden Faktoren ab:

- der Größe und der Erfahrung des internen IAM-Teams
- der Komplexität der vorhandenen Systeme und Integrationen
- dem durchschnittlichen Stundensatz (inkl. Nebenkosten) eines IAM-, Audit- und Compliance-VZÄs

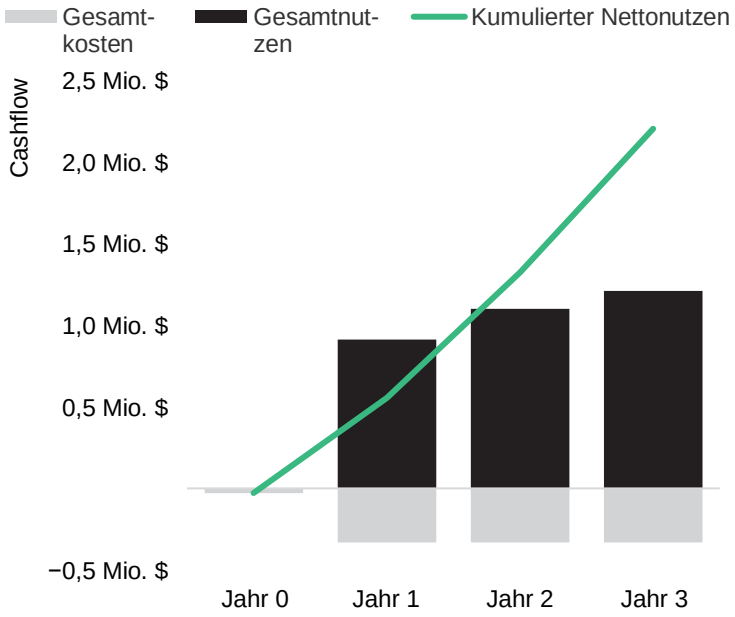
Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester die genannten Kosten um 10 % nach oben korrigiert. So ergibt sich über drei Jahren ein risikobereinigter Gesamtbarwert (abgezinst mit 10 %) von 28.000 USD.

Schulungen, Implementierung und Optimierung						
Ref.	**Kennzahl**	**Quelle**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**
G1	IAM-VZÄ und dedizierte Audit-/Compliance-VZÄ	Modellunternehmen	12			
G2	Integrationsphase (Wochen)	Befragungen	8			
G3	Durchschnittlich zugeteilte Zeit für OIG-Schulungen, Implementierung und/oder Optimierung von OIG	Befragungen	10 %			
G4	**Zwischensumme: für die OIG-Integration aufgewendeten Stunden**	**G1*G2*40*G3**	**384**			
G5	Durchschnittlicher Stundensatz (inkl. Nebenkosten) eines IAM-VZÄ und dedizierten Audit-/Compliance-VZÄs	Modellunternehmen	66 $			
Gt	Schulungen, Implementierung und Optimierung	G4*G5	25.344 $	0 $	0 $	0 $
	Risikobereinigung	↑ 10 %				
Gtr	Schulungen, Implementierung und Optimierung (risikobereinigt)		27.878 $	0 $	0 $	0 $
	Gesamtwert über drei Jahre: 27.878 $			**Barwert über drei Jahre: 27.878 $**		

Finanzergebnisse

Konsolidierte risikobereinigte Kennzahlen für einen Zeitraum von drei Jahren

Cashflow-Diagramm (risikobereinigt)



Die in den Nutzen- und Kostenabschnitten berechneten finanziellen Ergebnisse können zur Bestimmung des ROI, des Kapitalwerts und des Amortisationszeitraums für die Investition des Modellunternehmens genutzt werden. Forrester geht bei dieser Analyse von einem jährlichen Abzinsungssatz von 10 % aus.

Zur Ermittlung der risikobereinigten Werte für ROI, Kapitalwert und Amortisationszeitraum wurden Risikoanpassungsfaktoren auf die unbereinigten Ergebnisse der einzelnen Nutzen- und Kostenpositionen angewendet.

Cashflow-Analyse (risikobereinigt)

	Jahr 0	Jahr 1	Jahr 2	Jahr 3	Gesamt	Barwert
Gesamtkosten	(27.878 $)	(330.000 $)	(330.000 $)	(330.000 $)	(1.017.878 $)	(848.539 $)
Gesamtnutzen	0 $	911.173 $	1.096.688 $	1.208.320 $	3.216.181 $	2.642.522 $
Nettonutzen	(27.878 $)	581.173 $	766.688 $	878.320 $	2.198.303 $	1.793.983 $
Kapitalrendite						211 %
Amortisation						< 6 Monate

ANHANG A: TOTAL ECONOMIC IMPACT

Total Economic Impact ist eine von Forrester Research entwickelte Methodik, die die technologiebezogenen Entscheidungsprozesse eines Unternehmens optimiert und Anbieter bei der Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber ihrer Kundschaft unterstützt. Die Methodik des TEI hilft Unternehmen, den konkreten Mehrwert von IT-Initiativen gegenüber der Geschäftsleitung und anderen wichtigen Stakeholdern darzulegen, zu begründen und zu veranschaulichen.

Konzept des Total Economic Impact

Nutzen ist der Wert, den das Unternehmen aus dem Produkt zieht. Bei der Methodik des Total Economic Impact werden der Nutzen und die Kosten gleich gewichtet. Dadurch wird eine umfassende Untersuchung der Auswirkungen einer bestimmten Technologie auf das gesamte Unternehmen ermöglicht.

Kosten berücksichtigen alle Ausgaben, die notwendig sind, um den beabsichtigten Mehrwert oder Nutzen des Produkts zu erzielen. Die Kostenkategorie innerhalb des TEI erfasst die über das gegenwärtige Geschäftsumfeld hinausgehenden Mehrkosten für die mit der Lösung verbundenen laufenden Kosten.

Flexibilität stellt den strategischen Wert dar, der für weitere künftige Investitionen, die auf den bereits getätigten Anfangsinvestitionen aufbauen, erzielt werden kann. Die Möglichkeit, diesen Nutzen zu realisieren, stellt bereits einen Barwert dar, der prognostiziert werden kann.

Risiken messen die Ungewissheit von Nutzen- und Kostenschätzungen angesichts: 1) der Wahrscheinlichkeit, dass die Schätzungen den ursprünglichen Prognosen entsprechen, und 2) der Wahrscheinlichkeit, dass die Schätzungen im Laufe der Zeit mit den tatsächlichen Werten abgeglichen werden. Die Risikofaktoren des Total Economic Impact basieren auf einer „Dreiecksverteilung“.

Barwert (BW)

Der Barwert bzw. aktuelle Wert von (abgezinsten) Kosten- und Nutzenschätzungen mit einem gegebenen Zinssatz (dem Diskontierungssatz). Der Barwert für Kosten und Nutzen fließt in den Gesamtkapitalwert des Cashflows ein.

Kapitalwert (KW)

Der Barwert bzw. aktuelle Wert von (abgezinsten) zukünftigen Netto-Cashflows mit einem gegebenen Zinssatz (dem Diskontierungszinssatz). Ein positiver Projektkapitalwert bedeutet in der

Regel, dass die Investition empfehlenswert ist, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

Kapitalrendite (ROI)

Die erwartete Rendite eines Projekts in Prozent. Der ROI wird durch Division des Nettonutzens (Nutzen abzüglich Kosten) durch die Kosten berechnet.

Diskontierungssatz

Der in der Cashflow-Analyse verwendete Zinssatz, mit dem der Zeitwert des Geldes berechnet wird. Unternehmen verwenden in der Regel Diskontierungssätze zwischen 8 % und 16 %.

Amortisationszeitraum

Die Gewinnschwelle einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen abzüglich Kosten) gleich der Anfangsinvestition bzw. den Anfangskosten ist.

Die Spalte mit den Anfangsinvestitionen enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn von Jahr 1 anfallen und nicht abgezinst werden. Alle anderen Cashflows werden mit dem Diskontierungssatz zum Jahresende abgezinst. Die Barwertberechnungen werden für jede Gesamtkosten- und Gesamtnutzenschätzung vorgenommen. Die Berechnungen des Kapitalwerts in den Übersichtstabellen entsprechen der Summe der Anfangsinvestition und des abgezinsten Cashflows für die einzelnen Jahre. Die Summen und Barwertberechnungen in den Tabellen für Gesamtnutzen, Gesamtkosten und Cashflow ergeben möglicherweise nicht den exakten Gesamtwert, da einige Beträge eventuell gerundet sind.

ANHANG B: SCHLUSSBEMERKUNGEN

[1]Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methodik, die die technologiebezogenen Entscheidungsprozesse eines Unternehmens optimiert und Anbietern hilft, den Mehrwert ihrer Lösung verständlich zu machen. Sie hilft Unternehmen, den konkreten Wert von Wirtschafts- und Technologieinitiativen gegenüber der Geschäftsleitung und anderen wichtigen Stakeholdern darzulegen, zu rechtfertigen und zu veranschaulichen.

[2] Regressionsanalyse der gemeldeten kumulierten Gesamtkosten aller Sicherheitsverletzungen, die die Unternehmen der Sicherheitsentscheider in den letzten 12 Monaten erfahren haben. Der Umsatz des Modellunternehmens wird als Eingabe für die Regressionsformel verwendet. Quelle: Sicherheitsumfrage von Forrester, 2024. „Wie hoch sind Ihren Schätzungen nach die kumulierten Kosten aller Verstöße, die in Ihrem Unternehmen in den vergangenen 12 Monaten aufgetreten sind?“ Basis: 1.660 globale Sicherheitsentscheider, die in den letzten 12 Monaten von einer Sicherheitsverletzung betroffen waren.

[3] Regressionsanalyse der Wahrscheinlichkeit, mindestens eine Sicherheitsverletzung zu erleben, basierend auf der Häufigkeit von Sicherheitsverletzungen in den letzten 12 Monaten, wie von Sicherheitsentscheidern berichtet. Der Umsatz des Modellunternehmens wird als Eingabe für die Regressionsformel verwendet. Quelle: Sicherheitsumfrage von Forrester, 2024. „Wie oft kam es Ihrer Einschätzung nach in den letzten 12 Monaten in Ihrem Unternehmen zu einer potenziellen Kompromittierung oder Verletzung der Sicherheit Ihrer vertraulichen Daten?“ Basis: 2.769 globale Sicherheitsentscheider.

[4] Prozentsatz der Sicherheitsverletzungen nach primärem Angriffsvektor für Sicherheitsverletzungen, gemäß den Meldungen der Sicherheitsentscheider, deren Unternehmen in den letzten 12 Monaten mindestens eine Sicherheitsverletzung erlitten haben. Quelle: Sicherheitsumfrage von Forrester, 2024. „Geben Sie für die Vorfälle, bei denen es in den letzten 12 Monaten in Ihrem Unternehmen zu einer potenziellen Kompromittierung oder Verletzung der Sicherheit Ihrer vertraulichen Daten kam, bitte an, wie viele jeweils unter die folgenden Kategorien fallen.“ Basis: 1.542 globale Sicherheitsentscheider, die in den letzten 12 Monaten eine Sicherheitsverletzung erlebt haben.

FORRESTER®