The Total Economic Impact™ Of Okta Identity Governance

Cost Savings And Business Benefits Enabled By Identity Governance

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY OKTA, JUNE 2025

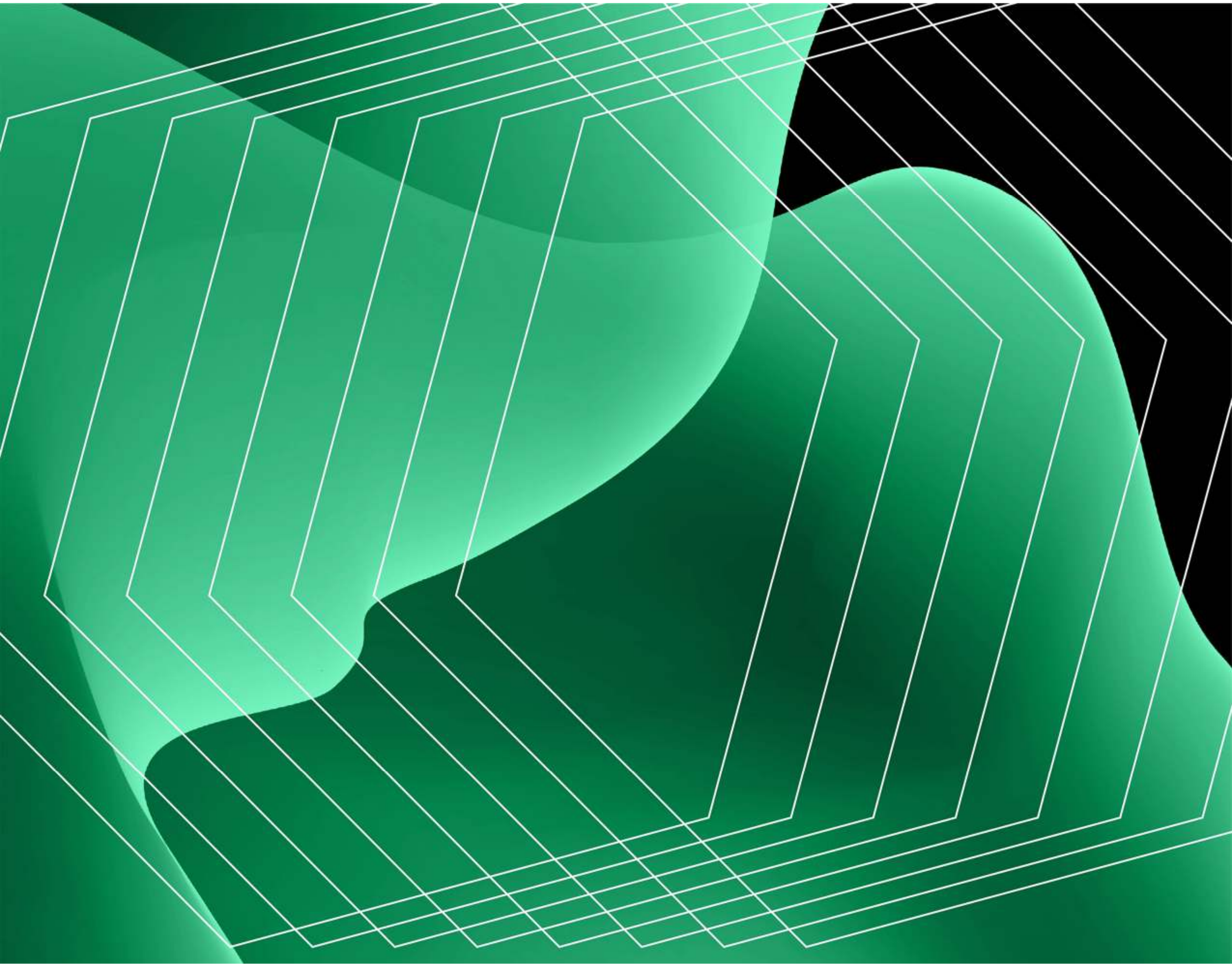


Table Of Contents

Consulting Team:

Kris Peterson

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Organizations of all sizes need a proactive, policy-driven approach to effectively manage access and entitlements — balancing agility and scalability with control, oversight, and compliance in the face of growing security threats and regulatory pressure, such as SOX and PCI-DSS. Disparate systems and manual processes often create blind spots, delay access provisioning, and contribute to overentitled users and excessive reporting efforts. As identity environments grow in scale and complexity, organizations need governance solutions that integrate with core identity infrastructure to support both operational efficiency and risk reduction.

Okta Identity Governance (OIG), a cloud-based identity governance and administration (IGA) solution, integrates directly with identity infrastructure to centralize and automate access requests, certifications, entitlement reviews, policy enforcement, and reporting. By replacing manual workflows with event-driven automations and dynamic access logic, OIG helps organizations enforce least-privilege access, accelerate provisioning and deprovisioning, and maintain compliance at scale — while minimizing administrative overhead and access risk.

Okta commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Okta Identity Governance.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Okta Identity Governance on their organizations.

Return on investment (ROI)

211%

Net present value

$1.8M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed eight decision-makers with experience using OIG. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization — a global enterprise with $1.5 billion in annual revenue, 5,000 identities, 100 applications, and 12 employees responsible for identity and access management (IAM), audit support, and compliance enforcement.

Interviewees said that prior to implementing OIG, their environments were heavily dependent on manual work, fragmented tools, and inconsistent access policies, resulting in inefficiencies, human errors, and security vulnerabilities. Previous attempts to formalize identity governance were often incomplete or unsustainable, leading to delayed provisioning, overentitled users, audit friction, and increased risk exposure.

After the investment in OIG, interviewees reported a shift from reactive oversight to proactive, policy-driven governance. IAM teams gained centralized visibility, automated key workflows, and enforced access controls more consistently — enabling faster service delivery, simplified audits, and a stronger security posture.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Improved identity governance efficiency worth $1.1 million.** Automating access requests, certification reviews, and entitlement management reduces the effort required by the composite's IAM and IT support teams by up to 60%. These savings reflect avoided manual work related to access reviews, entitlement hygiene, and ad hoc access requests, as well as the time saved by managers during access review and approval cycles.
- **Reduced audit preparation and compliance reporting efforts, totaling $232,000.** Improving access visibility and automating reviews simplify evidence collection and reduce the time required for the composite to respond to internal and external audit demands, including those related to SOX, PCI-DSS, and other regulatory frameworks. The composite organization also benefits from improved consistency in certification and access control workflows, helping avoid audit findings and strengthening its overall governance posture.
- **Enhanced platform efficiency and software rationalization, resulting in $567,000 in efficiency gains.** By replacing legacy tools and costly connectors with out-of-the-box integrations and by improving entitlement visibility, the composite avoids license and consulting costs while reducing the administrative effort tied to onboarding, offboarding, and access changes. Governance workflows automate key joiner-mover-leaver processes and enable policy-based enforcement without increasing staff headcount.

- **Increased productivity from access governance enhancements valued at $497,000.** End users, managers, and application owners at the composite spend less time navigating manual approval chains or chasing down access issues and spend more time on other, value-added business tasks. Even modest time savings per user can scale significantly across a large user base. Streamlined user experiences and consistent, audit-friendly workflows reduce delays and increase business agility.
- **Reduced risk of a security breach, worth a projected $231,000.** The composite organization reduces its measurable exposure to security breaches by strengthening its governance posture and eliminating excessive or outdated access. Governance automation and proactive entitlement reviews limit the risk of privilege misuse and insider threats while enabling a more consistent access policy footprint across systems.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Faster time to value.** Okta Identity Governance deploys rapidly compared with traditional IGA solutions. The composite organization sees immediate automation value, faster onboarding of users and applications, and a notably short ramp-up period — accelerating the realization of quantified benefits by weeks or months.
- **Improved IAM team morale.** Teams at the composite shift from performing manual, repetitive identity governance tasks to focusing on higher-value, strategic activities, such as policy design, exception handling, and roadmap planning.
- **Improved employee and end-user experience.** End users experience fewer access delays or disruptions, and managers spend less time reviewing or approving access certifications and requests. By enabling self-service access and streamlined approvals, the composite reduces friction and improves access to business-critical systems.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **OIG licensing fees of $821,000.** This reflects the total licensing cost for OIG functionality and standard support across a user base of 5,000 identities.
- **Implementation and deployment effort totaling $28,000.** This includes one-time setup, internal project management, and configuration work as well as light ongoing effort to maintain governance workflows and policies.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $2.6 million over three years versus costs of $849,000, adding up to a net present value (NPV) of $1.8 million and an ROI of 211%.

Total labor savings and efficiency gains in identity governance, audit, and compliance efforts and access governance enhancements

$1.8M

"[OIG] does everything it's supposed to do on day one and more. You get the capabilities you need to be compliant, and your users are happy. That says it all for me right there."

SENIOR DIRECTOR, GLOBAL HEAD OF IAM, PROFESSIONAL SERVICES

"If we look at the labor savings across all the users — whether it's service desk, security, audit, the application owners, and the business managers that have to review and approve access requests — the labor savings justify the cost overall. Then the reduction in risk to the organization and how it improves our security posture overall is a huge benefit as well."

CIO, FINANCIAL SERVICES

ROI

211%

BENEFITS PV

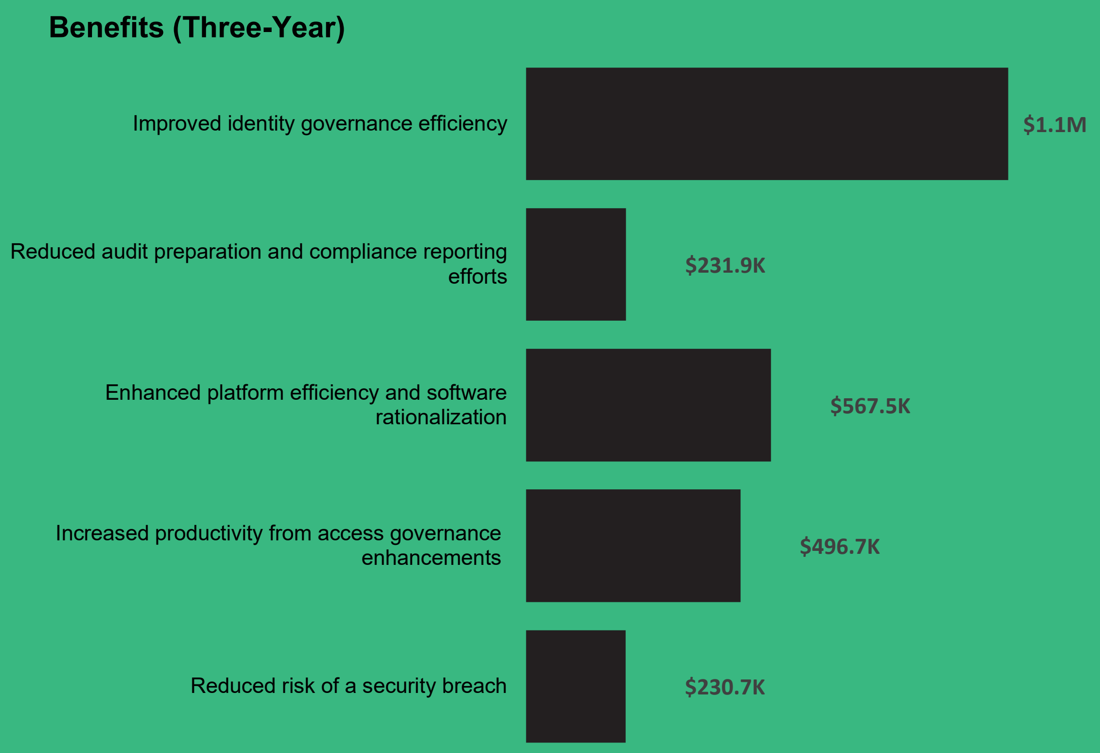
$2.6M

NPV

$1.8M

PAYBACK

<6 months



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Identity Governance.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Identity Governance can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Okta and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Identity Governance.

Okta reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Okta provided the customer names for the interviews but did not participate in the interviews.

1. **Due Diligence**
   Interviewed Okta stakeholders and Forrester analysts to gather data relative to Identity Governance.

2. **Interviews**
   Interviewed eight representatives at organizations using Identity Governance to obtain data about costs, benefits, and risks.

3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.

4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Okta Identity Governance Customer Journey

Drivers leading to the Identity Governance investment

Interviews

Role	Industry	Region	Identities/ managed apps
Director, IAM	IT services	Global; headquartered in North America	104,000/200
Director of security architecture	IT consultancy	Global; headquartered in North America	100,000/1,500
Managing director	Financial services	Global; headquartered in North America	70,000/90
Senior director, global head of IAM	Professional services	Global; headquartered in North America	8,000/400
CIO	Financial services	Global; headquartered in EMEA	8,000/100
Information security director	Healthcare	North America	7,200/370
IT solutions architect	Software	Global; headquartered in North America	3,000/70
CISO	IT services	EMEA	2,200/200

KEY CHALLENGES

Prior to deploying Okta Identity Governance, interviewees described fragmented identity environments shaped by a mix of legacy IGA platforms, homegrown tools, and manual processes. These environments created both operational inefficiencies for IT teams and compliance and access control gaps for security teams. Access requests were often ticket-based, certifications were spreadsheet-driven, and entitlement management lacked standardization. These limitations resulted in inconsistent user experiences and increased compliance risk; they also placed undue burden on IT and security personnel.

Interviewees highlighted several common challenges, including:

- **Manual provisioning and access changes that delayed productivity and created risk.** Many interviewees noted that access was granted or revoked via help desk tickets with SLA targets of five days or more; others added that users often retained inappropriate access long after role changes or offboarding, increasing the potential for privilege creep or insider risk. The IT solutions architect in software explained that access requests overwhelmed their team and they had to enlist other personnel to help: "We had about 30 folks in it. It would be spread out evenly among all of them because there's no way my little team of three IAM people could handle all the access requests coming in, so it was a joint venture."

- **Access certifications that were slow, labor-intensive, and error-prone.** Organizations relied heavily on spreadsheets and manual attestations to meet audit and compliance requirements. Multiple interviewees reported that certifications often required weeks of preparation by IAM personnel and hours of review time for managers and business owners. The information security director in healthcare characterized campaigns as a "miserable experience" and said: "We were never actually completing our certifications. They would fail mid-campaign because we would have so much pushback from leaders. They would refuse to do them, so we could never get to the point of saying that we were actually meeting our policy."
- **Entitlement management that lacked visibility and standardization.** Without centralized governance, role-based access was inconsistently applied and users frequently accumulated excessive or outdated entitlements. The senior director, global head of IAM in professional services explained that "people tend to hoard access" — and that their team had to manually flag and resolve overprovisioned accounts.
- **Audit preparation that required significant time and coordination.** Interviewees described audits as highly disruptive before OIG, often requiring weeks of preparation and multiple staff members to compile access logs, track review completions, and respond to audit findings.

> "Everybody dreaded when we would show up [before OIG], and now we're looked at as a business enabler. That's pretty powerful."
>
> IT SOLUTIONS ARCHITECT, SOFTWARE

> "We've taken away a lot of manual tasks that were prone to error and increased our accuracy on managing accounts and provisioning [with OIG], whether it's applications, users, or customers."
>
> CIO, FINANCIAL SERVICES

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global organization generates $1.5 billion in annual revenue and has 5,000 identities and 100 applications. The IAM team includes 10 FTEs covering identity engineering, governance operations, policy enforcement, and certification campaigns as well as two FTEs providing audit and compliance support. Prior to OIG, the organization uses Okta for core identity services alongside a separate legacy solution and manual processes for access governance.

Deployment characteristics. The composite organization deploys OIG components for access certification and requests, entitlement management, audit and compliance reporting, and automation via Okta Workflows during an eight-week implementation period at the outset of Year 1.

KEY ASSUMPTIONS

$1.5 billion in revenue

5,000 identities

An IAM team with 10 FTEs managing identity governance and two FTEs providing audit and compliance support

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Improved identity governance efficiency	$323,366	$475,538	$570,645	$1,369,548	$1,115,709
Btr	Reduced audit preparation and compliance reporting efforts	$69,401	$99,144	$115,668	$284,213	$231,932
Ctr	Enhanced platform efficiency and software rationalization	$225,900	$229,500	$229,500	$684,900	$567,460
Dtr	Increased productivity from access governance enhancements	$199,750	$199,750	$199,750	$599,250	$496,749
Etr	Reduced risk of a security breach	$92,757	$92,757	$92,757	$278,270	$230,672
	Total benefits (risk-adjusted)	$911,173	$1,096,688	$1,208,320	$3,216,181	$2,642,522

IMPROVED IDENTITY GOVERNANCE EFFICIENCY

Evidence and data. Interviewees described extensive manual processes for access certifications, entitlement management, and handling ad hoc access requests prior to deploying Okta Identity Governance.

- The director, IAM at an IT services organization talked about the emphasis their team put on automations and self-service capabilities. They explained that: “The volume [of IAM work that] was more than 36 [people] full time dedicated to doing the same kind of stuff that we have now happening with basically five [people with OIG]. … Through their capabilities and automation using Workflows, we’re not going and developing and building scaffolding to do this stuff. We are living within the Okta platform using their low-code/no-code Workflows to do the automations.”

- The director, IAM added that the organization runs between 80 and 90 campaigns a month, covering 20,000 to 80,000 items, that each take less than an hour of work for the IAM team.
- The information security director at a healthcare organization said: “On the infosec side, it used to take one engineer and one analyst about four weeks to prepare a campaign. Then they had to babysit it and handhold managers — sometimes several hundred at a time. Two resources were basically tied up a quarter of the year just running access reviews. … Setting one up now takes 30 minutes.”
- The CIO in financial services said, “We went from 50% automation to 90% automation [with OIG] [and a] 50% reduction in labor.”
- The senior director, global head of IAM at a professional services organization estimated their IAM team of nine is now doing the work of 14 to 15 people.
- The CISO in IT services identified the automation provided by OIG as a top benefit, explaining that the organization has “basically built everything on Workflows and automated processes to take away that manual effort.”
- The IT solutions architect at a software organization discussed the impact of Okta Workflows: “We did have automation in place, but it was a hodgepodge of everything — PowerShell scripts, Python scripts, AWS Lambda functions, just all over the place. We were able to migrate all of that into the Okta Workflow stack and then use the built-in hooks into all of our different identity-related operations, which drastically reduced the complexity and also the amount of time needed to maintain those different platforms.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Ten IAM FTEs are allocated to core identity governance tasks, such as access requests and reviews and entitlement management.
- The average fully burdened annual salary of an IAM FTE is $140,900.
- After the eight-week implementation period, the team saves 40% of the time spent on identity governance tasks for the remaining 44 weeks, for a net savings in Year 1 of 34%.
- The time saved increases to 50% in Year 2 and 60% in Year 3 as more applications are managed by OIG and more automations are integrated, further reducing prior manual efforts.

- These time savings are reallocated toward other value-added activities at a rate of 75%.

Risks. To support realistic and defensible estimates, Forrester applies risk adjustments based on the consistency of interview evidence and the degree of variation in reported outcomes. This component of TEI methodology helps account for differences in implementation environments. The amount of this benefit can vary across customers due to differences in:

- The level of automation and time savings, which may vary based on legacy system complexity or compliance requirements.
- The need for manual oversight, which may be greater in organizations with regulatory or industry-specific constraints.
- The scale of benefit, which depends on user volume, campaign frequency, and the number and complexity of applications governed.
- The average fully burdened annual salary of an IAM FTE.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.1 million.

Time saved on identity governance tasks by Year 3

60%

> “We’re doing close to 10 times the work that we did when it was just [the legacy solution], easily — maybe even more than that.”
>
> INFORMATION SECURITY DIRECTOR, HEALTHCARE

> "Workflows save a lot of FTEs. Given the number of applications we have, it would otherwise be almost impossible to manage."
>
> DIRECTOR OF SECURITY ARCHITECTURE, IT CONSULTANCY

Improved Identity Governance Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	IAM FTEs allocated to access requests and reviews, entitlement management, and other identity governance tasks	Composite	10	10	10
A2	Fully burdened annual salary of an IAM FTE with identity governance tasks	Composite	$140,900	$140,900	$140,900
A3	Net time saved after implementation of OIG for identity governance tasks	Interviews	34%	50%	60%
A4	Productivity recapture	TEI methodology	75%	75%	75%
At	Improved identity governance efficiency	A1*A2*A3*A4	$359,295.0	$528,375.0	$634,050.0
	Risk adjustment	↓10%			
Atr	Improved identity governance efficiency (risk-adjusted)		$323,365.50	$475,537.50	$570,645.00
	Three-year total: $1,369,548		**Three-year present value: $1,115,709**		

REDUCED AUDIT PREPARATION AND COMPLIANCE REPORTING EFFORTS

Evidence and data. Interviewees reported that OIG helps streamline or avoid significant manual effort related to recurring audits, access reviews, and compliance reporting. Teams previously responsible for validating access controls and preparing evidence and reports reported material time savings and reduced audit-related efforts. Specific areas of reduced or avoided effort included the following.

- Interviewees described the weeks of audit preparation effort needed before OIG, which involved manually gathering certification data, taking screenshots of access approvals, and validating access control logs across systems.

- Several interviewees noted that automated certification workflows improved the completeness and consistency of review processes, reducing the risk of missing or incorrect records that could trigger findings. They also identified centralized policies, workflows, and audit logs in OIG as factors in reducing the effort required to explain governance processes to auditors and document exceptions.
- Interviewees described saving time and reducing complexity by using OIG dashboards to generate ad hoc reports on access reviews, user roles, and entitlements. These features helped teams respond more quickly to internal audit or external regulatory inquiries.
- The senior director, global head of IAM in professional services explained that without OIG's automation, they "would have needed a team of three to five people to manage the consistency" of evidence gathering.
- The senior director added: "I am able to present to an auditor in a single 30-minute session and be done. Zero follow-up. … [The auditor] came back to me with [a request for their] security engineer to reach out to [us] so that [they] could implement [OIG]. That has happened twice. … That's like the biggest compliment ever."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Audit and compliance tasks are allocated to two FTEs.
- The average fully burdened annual salary of an audit and compliance FTE is $122,400.
- After the eight-week implementation period, the team saves 50% of the time spent on audit preparation and compliance reporting tasks for the remaining 44 weeks, for a net savings in Year 1 of 42%.
- The time saved increases to 60% in Year 2 and 70% in Year 3 as the IAM team becomes more efficient and OIG governance expands.
- These time savings are reallocated toward other value-added activities at a rate of 75%.

Risks. The amount of this benefit can vary across customers due to differences in:

- The number and complexity of audits required based on industry and geography.
- The maturity of existing processes and tools prior to adopting OIG.
- The size and structure of the IAM and compliance teams.

- The degree to which audit-related tasks are automated or integrated into other governance systems.
- The average fully burdened annual salary of an audit and compliance FTE.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $232,000.

Time saved on audit and compliance tasks by Year 3

70%

Reduced Audit Preparation And Compliance Reporting Efforts

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	IAM FTEs with audit and compliance tasks	Composite	2	2	2
B2	Fully burdened annual salary of an IAM FTE with audit and compliance tasks	Composite	$122,400	$122,400	$122,400
B3	Net time saved on audit and compliance tasks with OIG	Interviews	42%	60%	70%
B4	Productivity recapture	TEI methodology	75%	75%	75%
Bt	Reduced audit preparation and compliance reporting efforts	B1*B2*B3*B4	$77,112.00	$110,160.00	$128,520.00
	Risk adjustment	↓10%			
Btr	Reduced audit preparation and compliance reporting efforts (risk-adjusted)		$69,400.80	$99,144.00	$115,668.00
	Three-year total: $284,213		**Three-year present value: $231,932**		

ENHANCED PLATFORM EFFICIENCY AND SOFTWARE RATIONALIZATION

Evidence and data. Interviewees shared that Okta Identity Governance improved platform efficiency by reducing reliance on costly external consultants, eliminating custom connectors, and empowering internal teams with low-code/no-code tools. In parallel, organizations gained better entitlement visibility and usage insights, allowing them to rationalize software spend and remove unused licenses. Together, these changes enhanced operational efficiency and strengthened governance coverage.

Platform efficiency:

- The information security director in healthcare reported that before OIG, their organization was spending $150,000 to $200,000 annually on consultants to make progress on legacy solution initiatives. With OIG, that additional cost is no longer needed thanks to out-of-the-box connectors, low-code/no-code automations, and internal resources empowered by more modern tooling.
- The CIO in financial services added: “[OIG] comes with a lot of prebuilt integrations, so that made it easier to connect to our current environment. … [OIG is also] helping us realize a benefit around license and resource management because of less unused accounts.”
- The senior director, global head of IAM noted that their professional services firm paid $15,000 to $25,000 to connect applications and as a result: “You don’t connect all the systems that you would have connected [for] governance, so there’s a risk that you have gaps because they’re not connected via an API…. [With OIG], anything that had SSO connected to my identity provider automatically got added into governance, as it should be.”

Software rationalization:

- Interviewees explained that OIG’s entitlement visibility helped identify and remove unused or duplicate licenses. The IT solutions architect said their software firm conducts ad hoc certification campaigns to gain real-time insight on who is actually using applications and has “seen a huge benefit every time we roll it out.” One example reduced approximately 200 licenses for an application with 550 users at a cost of $5 to $10 per user per month.
- When asked about savings related to platform efficiencies and software rationalization, the CIO at a financial services firm estimated their organization saves over $200,000 annually.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The organization connects 10 incremental applications using OIG that would have required a paid connector under the legacy solution.

- Connector fees are $20,000 per application.
- OIG enables license cleanup for 10 applications, with an average of 50 unused or duplicative licenses removed and a monthly cost of $5 per license.
- After the eight-week implementation period, the organization avoids $21,000 in consulting or third-party support in Year 1 and $25,000 in Years 2 and 3.

Risks. The amount of this benefit can vary across customers due to differences in:

- The cost and availability of prebuilt connectors for legacy IGA solutions.
- The number and types of applications added or governed via OIG.
- License structures and overprovisioning patterns across enterprise software environments.
- Reliance on external consultants or managed service providers for IAM functions.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $568,000.

Enhanced Platform Efficiency And Software Rationalization

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Legacy solution connector fees per application	Interviews	$20,000	$20,000	$20,000
C2	Incremental application connections enabled by OIG	Composite	10	10	10
C3	**Subtotal: Avoided connector fees with OIG**	**C1*C2**	**$200,000**	**$200,000**	**$200,000**
C4	Applications with license cleanup enabled by OIG	Composite	10	10	10
C5	Unnecessary licenses removed per application	Interviews	50	50	50
C6	Average monthly license cost per user	Interviews	$5	$5	$5
C7	**Subtotal: Avoided license fees with OIG**	**C4*C5*C6*12**	**$30,000**	**$30,000**	**$30,000**
C8	Avoided consulting/third-party support costs for IAM	Interviews	$21,000	$25,000	$25,000
Ct	Enhanced platform efficiency and software rationalization	C3+C7+C8	$251,000.00	$255,000.00	$255,000.00
	Risk adjustment	↓10%			

Ctr	Enhanced platform efficiency and software rationalization (risk-adjusted)	$225,900	$229,500	$229,500
	Three-year total: $684,900		**Three-year present value: $567,460**	

INCREASED PRODUCTIVITY FROM ACCESS GOVERNANCE ENHANCEMENTS

Evidence and data. Interviewees described how OIG streamlined access-related workflows for end users, managers, and application owners. Before OIG, end users would often over-request, resulting in delays and extra follow-up. With OIG, requests are routed and resolved more efficiently, reducing the burden on requesters and approvers. Automating and simplifying access requests, certifications, and entitlement reviews helped reduce the time spent navigating outdated interfaces, waiting on manual approvals, or responding to inconsistent governance processes.

- The IT solutions architect in software said: "[Before OIG], it would be between 45 minutes to 2-hour-long processes to get the approvals done, and up to 24 hours for access to be granted. We were able to collapse that with 30 minutes [to] when the request is fully completed end to end."
- The managing director in financial services said about access requests or changes, "[It] would take at least the SLA of five business days, and now it's automated and done within 30 minutes."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- 5,000 end users save, on average, 2 hours per year with OIG as a result of fewer access issues and improved access approvals and provisioning.
- The average fully burdened hourly rate of an end user is $47.

Risks. The amount of this benefit can vary across customers due to differences in:

- The types and volume of access-related tasks assigned to business users.
- The maturity and consistency of governance workflows prior to implementing OIG.
- The level of automation and customization deployed during rollout.
- How widely the request and certification workflows are adopted across the organization.
- The average fully burdened hourly rate of an end user.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $497,000.

Value of time saved for end users from access governance enhancements

$497,000

> “[OIG] drastically improves the user experience. They can get what they need done very quickly [and] move on to work and what they actually are doing for their job, versus before [when] it would take a lot of productivity away from them.”
>
> MANAGING DIRECTOR, FINANCIAL SERVICES

Increased Productivity From Access Governance Enhancements

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Total end users	Composite	5,000	5,000	5,000
D2	Average hours saved per end user from improved access approvals and provisioning and fewer access issues with OIG	Interviews	2	2	2
D3	Fully burdened hourly rate of an end user	Composite	$47	$47	$47
D4	Productivity recapture	TEI methodology	50%	50%	50%
Dt	Increased productivity from access governance enhancements	D1*D2*D3*D4	$235,000	$235,000	$235,000
	Risk adjustment	↓15%			
Dtr	Increased productivity from access governance enhancements (risk-adjusted)		$199,750	$199,750	$199,750
	Three-year total: $599,250		Three-year present value: $496,749		

REDUCED RISK OF A SECURITY BREACH

Evidence and data. Interviewees confirmed that Okta Identity Governance helped reduce the risk of a security breach by enforcing least-privilege access, eliminating unnecessary entitlements, and automating reviews and removals. Several highlighted OIG's role in curbing access creep and cleaning up legacy access, which they noted as a foundational capability in their journey toward a Zero Trust architecture.

- The senior director, global head of IAM at a professional services firm said OIG helped reduce overprovisioned access and minimize human error, which previously exposed the organization to unnecessary risk. "People love that separation of duties and toxic entitlements. … The automation [from OIG] goes and looks quickly at the roles that you have to make sure the role that you're requesting isn't toxic to one of the ones you already have and remediate before it starts. It's a huge, massive deal."
- The information security director in healthcare explained that OIG facilitated a significant reduction in risk exposure related to protected health information (PHI). OIG helped tighten governance around PHI access, ensuring only essential users had visibility into sensitive data. This targeted reduction in unnecessary access mitigated potential compliance and security risks.
- The CIO in financial services said: "Having a capability to do separation of duties and policy enforcements helps us prevent conflict of interest and reduce potential fraud. … We've seen a reduction in insider threats because we've got a lot more visibility into these access reviews and certifications, especially with contractors and third-party partners. The automation of deprovisioning ensures that we're not leaving access for former employees or former contractors or vendors that have departed, so that's reduced a risk for us."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite faces an annual breach risk exposure of $3.027 million.[2] It has a likelihood of experiencing one or more breaches of 63%.[3]
- Of these breaches, 76% originate from external attacks or internal incidents or are related to the external ecosystem.[4]

- Eighty percent of those incidents are addressable through stronger identity governance and access controls provided by OIG.
- The composite reduces its exposure to these risks by 10% through the adoption of OIG, based on interviewee-reported improvements in access hygiene and review effectiveness.

Risks. The amount of this benefit can vary across customers due to differences in:

- Organizational size, industry, and inherent security risk profile.
- Existing identity governance maturity and tooling.
- The breadth of the OIG deployment and enforcement of access policies.
- The internal alignment between IAM, security, and compliance teams.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $231,000.

> "We've dramatically improved our security posture, which makes our CISO, compliance and risk teams, customers, and shareholders happy. [OIG] has a lot of benefit from a security perspective."
>
> CIO, FINANCIAL SERVICES

Reduced Risk Of A Security Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Cumulative cost of breaches for the composite	Forrester research	$3,027,000	$3,027,000	$3,027,000
E2	Likelihood of experiencing one or more breaches for the composite	Forrester research	63%	63%	63%
E3	Percent of breaches originating from external attacks targeting organizations, internal incidents, or involve the external ecosystem	Forrester research	76%	76%	76%

E4	Percent of those attacks addressable with OIG	Forrester research	80%	80%	80%
E5	**Subtotal: Annual risk exposure addressable with OIG**	**E1*E2*E3*E4**	**$1,159,462.0**	**$1,159,462.0**	**$1,159,462.0**
E6	Reduced risk of exposure to breach costs from addressable attacks with OIG	Interviews	10%	10%	10%
Et	Reduced risk of a security breach	E5*E6	$115,946	$115,946	$115,946
	Risk adjustment	↓20%			
Etr	Reduced risk of a security breach (risk-adjusted)		$92,757	$92,757	$92,757
	Three-year total: $278,270		**Three-year present value: $230,672**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Rapid time to value.** Interviewees consistently emphasized the speed with which they were able to deploy and derive value from OIG compared with traditional IGA platforms that often required months of planning, customization, and integration work. OIG enabled teams to stand up core capabilities — including access requests and certification workflows — with minimal resources and configuration effort. This accelerated ramp allowed organizations to begin realizing meaningful governance improvements almost immediately, even before full optimization or broad rollout.

  The CIO at a financial services organization noted that OIG delivered faster time to value due to its deep integration with the organization's existing Okta infrastructure — including single sign-on, multifactor authentication, and API access management. Because these core services were already in place, OIG could be deployed more quickly and with fewer integration hurdles compared with competing solutions.

  The information security director in healthcare said: "The implementation time was next to nothing. … There's nothing to really do. It's just part of the [Okta] platform. … We had it in production within two weeks — that was a grand slam for us."

  The senior director, global head of IAM at a professional services organization discussed the deployment process: “It was me and my two engineers at the time and that was it, just talking through on the call on a Thursday and Friday, and I looked up and realized this thing is done. We have access requests. We have governance and certifications that are spinning now. Let’s move this to prod. We could have had it done within the first day if we had had more confidence in our ability.”

- **Improved IT and security team morale.** The interviewees said that by eliminating repetitive manual tasks and reducing the administrative burden of managing access requests and certifications, OIG allowed their teams to focus on more strategic, higher-value work. Interviewees described this as a productivity *and* culture boost for IT, IAM, and security teams. The director of security architecture in IT consultancy said, “Now we have less manual process management, and it allows us to focus on more strategic goals.” The senior director, global head of IAM at a professional services organization said: “My guys are now pseudo-stepping up into other roles that they dreamt of and that they want to do but just didn’t have the resume for. [OIG] permits a leader to prioritize work differently because you’re giving it to a team member that not only wants to do it as an analyst — they have the desire to do it. They’re knocking at your door, begging to get this kind of work. It’s the cool work.”

> “The expertise [Okta] provides is very commendable. I really enjoy working with them. Their customer success and support people really know what they’re talking about.”
>
> MANAGING DIRECTOR, FINANCIAL SERVICES

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Identity Governance and later realize additional uses and business opportunities, including:

- **Increased future-readiness and agility.** Interviewees cited OIG’s flexibility as a key enabler of both near-term wins and long-term strategic growth. Several interviewees noted that they started with a narrow use case — such as access requests or onboarding — and then expanded coverage over time to additional applications, business units, or compliance frameworks. Interviewees described this phased approach as essential for aligning governance scope with internal readiness and evolving regulatory priorities. OIG's native integration with Okta's identity platform allowed interviewees' organizations to scale without adding an administrative burden or disrupting existing workflows; controls could also be configured to support diverse geographies and standards (e.g., SOX, HIPAA, and ISO). The information security director in healthcare summarized it simply: "[With OIG,] you're in control of your own destiny."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> "The tool, the support, the mechanism that they've put in place to support the tool — it's uber-flexible."
>
> SENIOR DIRECTOR, GLOBAL HEAD OF IAM, PROFESSIONAL SERVICES

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	OIG fees	$1,100,000	$1,100,000	$1,100,000	$1,100,000	$4,400,000	$3,835,537
Etr	Training, implementation, and optimization	$0	$82,500	$165,000	$247,500	$495,000	$397,314
	Total costs (risk adjusted)	$1,925,000	$1,388,750	$1,265,000	$1,347,500	$5,926,250	$5,245,351

OIG FEES

Evidence and data. Interviewees provided cost details that were corroborated by Okta. For the composite organization, a cost estimate of $5 per user per month is based on the specific implementation and scenario related to the composite organization. Actual present value costs will vary based on the services provided with Okta and OIG to a particular customer. Contact Okta for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- OIG is deployed for 5,000 managed identities.
- The monthly fee is $5 per identity.

Risks. This cost can vary across customers due to differences in the negotiated pricing and licensing structure.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $821,000.

OIG Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Identities managed with OIG	Composite		5,000	5,000	5,000
F2	OIG monthly fees per identity	Interviews		$5	$5	$5
Ft	OIG fees	F1*F2*12	$0	$300,000	$300,000	$300,000
	Risk adjustment	↑10%				
Ftr	OIG fees (risk-adjusted)		$0	$330,000	$330,000	$330,000
	Three-year total: $990,000		**Three-year present value: $820,661**			

TRAINING, IMPLEMENTATION, AND OPTIMIZATION

Evidence and data. Interviewees noted that some training, implementation, and optimization activities were required to configure OIG, train personnel, and fine-tune access workflows. The duration of these activities ranged from weeks to a few months.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization.

- The IAM team and dedicated audit and compliance support staff spend eight weeks implementing OIG, allocating an average of 10% of time to OIG-specific tasks.
- The average fully burdened hourly rate of an IAM and audit and compliance FTE is $66.

Risks. The amount of this cost can vary across customers due to differences in:

- The size and experience level of the internal IAM team.
- The complexity of existing systems and integrations.
- The average fully burdened hourly rate of an IAM and audit and compliance FTE.

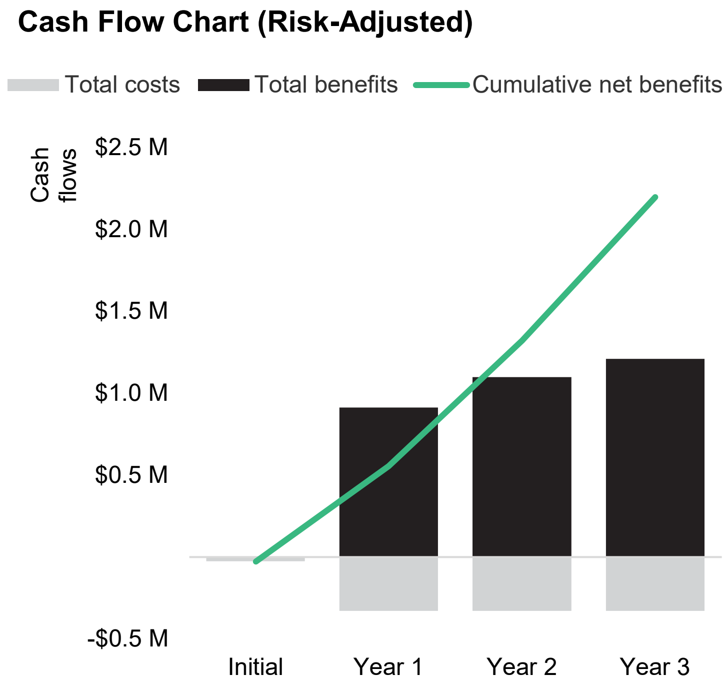
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $28,000.

Training, Implementation, And Optimization

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	IAM FTEs and dedicated audit/compliance FTEs	Composite	12			
G2	Integration period (weeks)	Interviews	8			
G3	Average time allocated to OIG training, implementation, and/or optimization	Interviews	10%			
G4	**Subtotal: Hours spent on OIG integration**	**G1*G2*40*G3**	**384**			
G5	Fully burdened hourly rate of an IAM and dedicated audit/compliance FTE	Composite	$66			
Gt	Training, implementation, and optimization	G4*G5	$25,344	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Training, implementation, and optimization (risk-adjusted)		$27,878	$0	$0	$0
	Three-year total: $27,878			**Three-year present value: $27,878**		

Financial Summary

Consolidated Three-Year Risk-Adjusted Metrics



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($27,878)	($330,000)	($330,000)	($330,000)	($1,017,878)	($848,539)
Total benefits	$0	$911,173	$1,096,688	$1,208,320	$3,216,181	$2,642,522
Net benefits	($27,878)	$581,173	$766,688	$878,320	$2,198,303	$1,793,983
ROI						211%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

Present Value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net Present Value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

Return on investment (ROI)

A project’s expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

The initial investment column contains costs incurred at “time 0” or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

APPENDIX B: ENDNOTES

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company’s technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

[2] Regression analysis of the reported total cumulative costs of all breaches experienced by security decision-makers’ organizations in the past 12 months. The composite organization’s revenue is used as the input to the regression formula. Source: Forrester’s Security Survey, 2024. “Using your best estimate, what was the total cumulative cost of all breaches experienced by your organization in the past 12 months?” Base: 1,660 global security decision-makers who have experienced a breach in the past 12 months.

[3] Regression analysis of the likelihood of experiencing one or more breaches, using the frequency that organizations experienced breaches in the past 12 months as reported by security decision-makers. The composite organization’s revenue is used as the input to the regression formula. Source: Forrester’s Security Survey, 2024. “How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?” Base: 2,769 global security decision-makers.

[4] Percent of breaches by primary attack vector for breaches, as reported by security decision-makers whose organizations experienced at least one breach in the last 12 months. Source: Forrester’s Security Survey, 2024. “Of the times that your organization's sensitive data was potentially compromised or breached in the past 12 months, please indicate how many of each fall into the categories below.” Base: 1,542 global security decision-makers who have experienced a breach in the past 12 months.

FORRESTER®