The Total Economic Impact™ Of Sectigo Certificate Manager

Cost Savings And Business Benefits Enabled By Sectigo Certificate Manager

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY
COMMISSIONED BY SECTIGO, AUGUST 2024

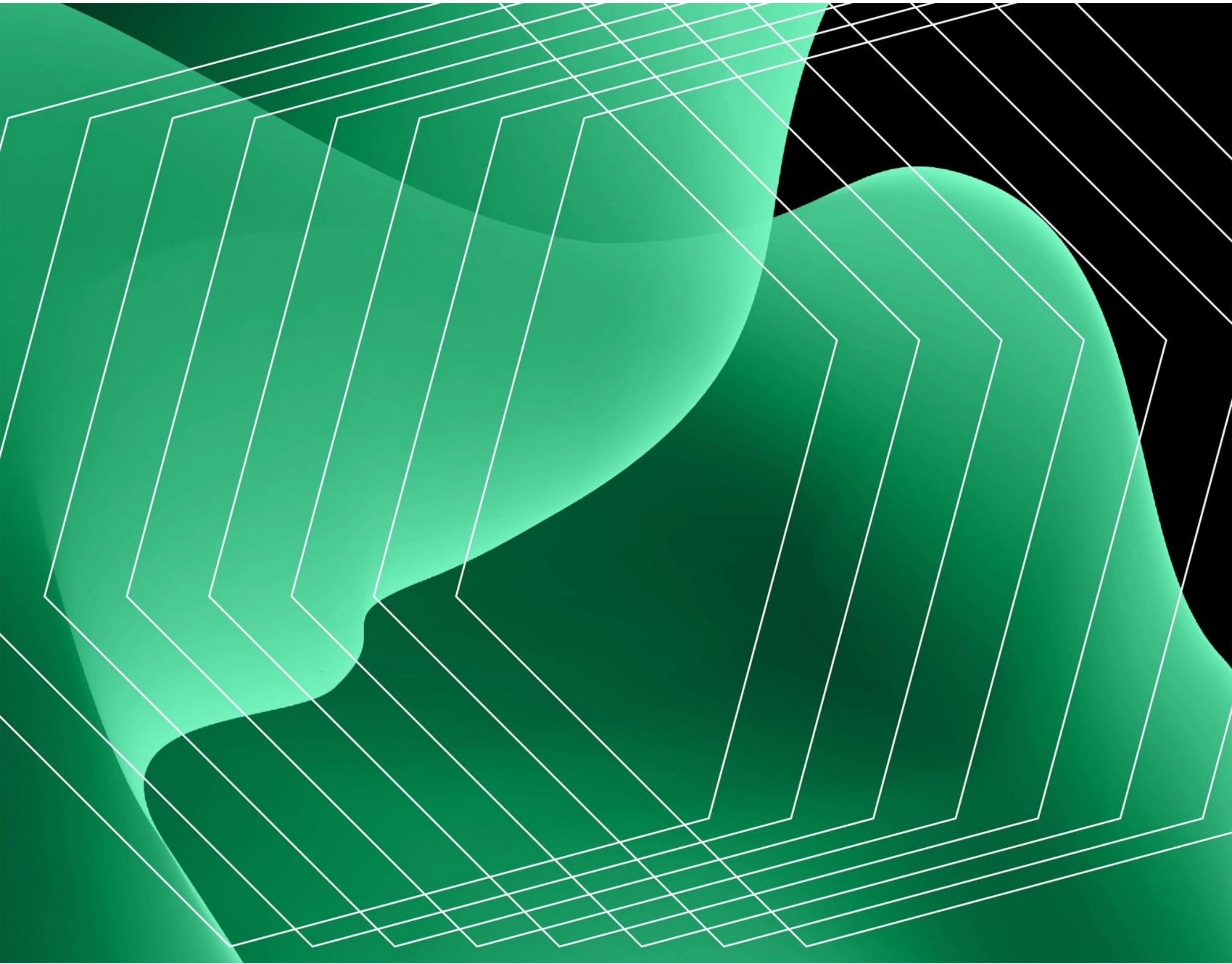


Table Of Contents

Consulting Team:

Roger Nauth

Eric Hall

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

The rising complexity and frequency of digital certificate renewals have significantly increased the risk of costly outages, underscoring the market demand for certificate lifecycle management (CLM) across businesses of all sizes. The CLM market continues to experience robust growth despite facing recent challenges due to one certificate authority (CA) failing to adhere to security standards regarding the certificates they issue. This growth is driven by increased enterprise investments and adoption by small to medium-sized businesses. Meanwhile, the trend towards 90-day issuance for public certificates further amplifies the need for effective CLM platforms, as organizations must continuously manage and renew their digital certificates to maintain operational continuity and efficiently safeguard their digital assets, underscoring the necessity for automated solutions.

The Sectigo Certificate Manager (SCM) vendor solution is a cloud-native CLM platform designed to automate the management of digital certificates and provide comprehensive visibility and control over certificate lifecycles. It addresses the key issue of time-consuming and brittle manual processes that are susceptible to human errors and the risk of costly outages. This issue is exacerbated by the increasing frequency of certificate renewals. The Sectigo solution uniquely supports crypto agility and integrates with various public and private certificate authorities, simplifying the user experience and enhancing security for businesses of all sizes. With over 50 integrations, Sectigo ensures interoperability, making it a comprehensive CLM solution.

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

Return on investment (ROI)

243%

Net present value (NPV)

$3.39M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives with experience using SCM. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. This composite organization is a global enterprise with a revenue of $37 billion and approximately 128,000 employees, of which around four FTEs manage about 100,000 certificates.

Interviewees said that prior to using SCM, their organizations relied heavily on manual processes for managing certificates, which were time-consuming and prone to human error. However, prior attempts to automate certificate management yielded limited success, leaving them with fragmented systems and a lack of centralized oversight. These limitations led to significant security vulnerabilities, frequent certificate expirations, and increased operational inefficiencies.

After the investment in SCM, the interviewees reported a significant improvement in their organizations' certificate management processes with automated workflows, centralized control, and enhanced security measures. Key results from the investment include a notable decrease in certificate-related outages, increased efficiency in managing certificates due to reduced manual tasks, and better compliance with security policies and regulations.

KEY FINDINGS

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

- **Reduced cost of legacy solutions and certificate authority costs worth $119,000 over three years.** The composite organization eliminates the use of legacy solutions, leading to cost reductions in licensing, IT maintenance, IT solution hosting, and training. Additionally, purchasing certificates from other certificate authorities is no longer necessary.
- **Provisioning labor cost reduction worth $1.3 million over three years.** On average, provisioning certificates with legacy solutions requires slightly more effort than with Sectigo. Manual provisioning took the composite organization significantly more time. The composite's certificate requirements were growing

rapidly, and its legacy solutions could not scale to provision a significant percentage of new certificates.

- **Renewal labor cost reduction worth $965,000 over three years.** The composite organization experiences shortened renewal frequency every year after implementing Sectigo. This reduction in frequency is expected to continue due to anticipated 90-day renewal requirements.
- **Reduced outage costs worth $2.4 million over three years.** Automation provided by Sectigo significantly reduces the risk of certificate-related outages by ensuring certificates are automatically renewed, while SCM's tracking capabilities enable teams to quickly respond to and resolve certificate-related problems.

Unquantified benefits. Benefits that provide value for the interviewees' organizations but are not quantified for this study include:

- **Risk reduction and security.** Interviewees noted the risk of errors and breaches was reduced due to Sectigo's management of the signing authority and the elimination of manual certificate management tasks. Additionally, their organizations no longer needed physical hardware security modules (HSMs) due to their use of Sectigo's managed services, reducing the associated risks and costs of these modules.
- **Sectigo partnership.** Interviewees noted Sectigo provided proactive and reactive support.
- **Certificate lifecycle management.** According to interviewees, certificate lifecycle management has improved. The interviewees noted their organizations can handle a high volume of certificates with fewer employees.
- **Ownership at the source.** With SCM, interviewees' organizations was able to give some teams to install, monitor, and renew their own certificates. This reduced the workload for IT.
- **Reporting, notifications, and exploring.** Interviewees noted they had increased confidence in their organizations' certificate tracking because of Sectigo's reporting capabilities. With SCM, expiration notices were sent to certificate owners at scheduled times before expirations.

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

- **Sectigo implementation costs.** The composite organization incurs initial costs for the setup and integration of Sectigo's certificate management solutions. This includes $20,000 for customer-specific implementation and $56,000 for Sectigo professional services. The implementation process spans approximately two months, involving significant coordination across multiple departments and initial training sessions to ensure smooth integration and user proficiency. The risk-adjusted cost for the initial setup is $83,600.
- **Implementation services, licensing, and premier services costs.** In addition to initial setup costs, the composite organization incurs ongoing costs for implementation services, licensing, and premier services. In Year 1, these costs total $469,700, which includes $378,000 for Sectigo licenses and $49,000 for premier services. These costs cover the development, customization, and automation of the certificate management system, as well as continued support and maintenance. Over three years, the risk-adjusted total cost for these services amounts to $1.6 million.

The representative interviews and financial analysis found that a composite organization experiences benefits of $4.78 million over three years versus costs of $1.39 million, adding up to a net present value (NPV) of $3.39 million and an ROI of 243%.

Total three-year, risk-adjusted present value (PV) costs for implementing Sectigo's certificate management solutions

$1.3 million

> “The implementation of Sectigo’s certificate management solutions not only streamlined our processes but also significantly reduced our overall operational costs.”
>
> SENIOR MANAGER OF CYBERSECURITY, BROADCASTING AND CABLE

Return on investment (ROI)

243%

Benefits PV

$4.78M

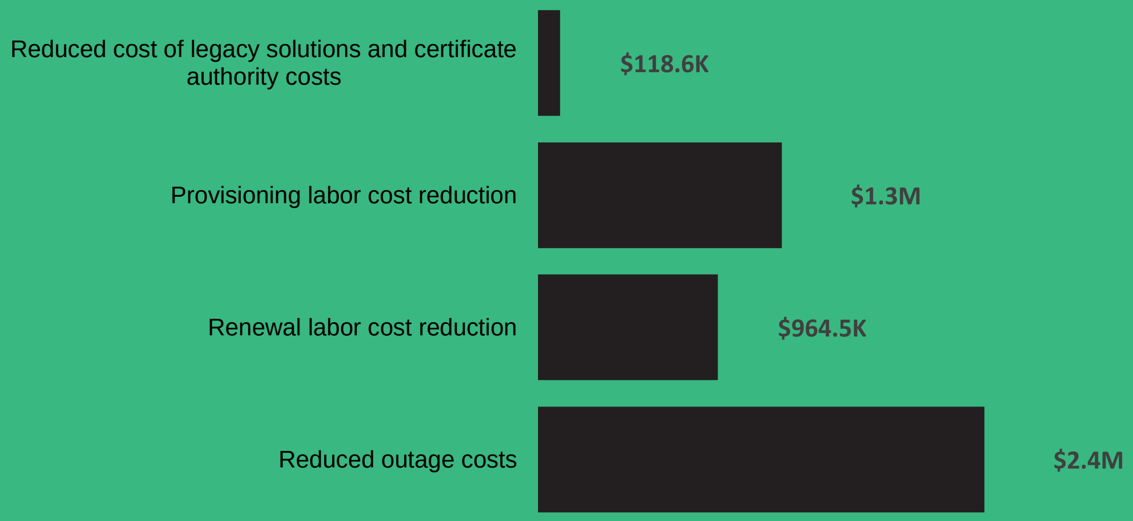
Net present value (NPV)

$3.39M

Payback

<6 months

Benefits (Three-Year)



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 SCM.

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 SCM can have on an organization.

DISCLOSURES
Readers should be aware of the following:

This study is commissioned by Sectigo 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 SCM.

Sectigo 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.

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

Due Diligence
Interviewed Sectigo stakeholders and Forrester analysts to gather data relative to SCM.

Interviews
Interviewed five representatives at organizations using SCM to obtain data about costs, benefits, and risks.

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

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.

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 Sectigo Certificate Manager Customer Journey

Drivers leading to the SCM investment

Interviews

Role	Industry	Headquarters	Revenue	Geographic Market	Employees
Information security manager	Logistics	United States	$25B	Global	500,000
Senior technology manager	Financial services/insurance	Canada	$150M	North America	8,500
Principal, global cybersecurity services	Financial services/insurance	Canada	$37B	North America	38,000
Senior manager of cybersecurity	Broadcasting and cable	United States	$122B	Global	73,000
Director of shared services	Payment and transactional services	France	$1.25B	Europe	18,000

KEY CHALLENGES

Before implementing SCM, the interviewees' organizations often faced significant challenges in managing their digital certificates. Typically, these prior solutions involved manual processes and disparate tools, leading to inefficiencies and a higher risk of errors. Certificates were often managed using spreadsheets or fragmented systems that lacked automation, making it difficult to track expiration dates and ensure timely renewals. This environment resulted in frequent incidents of expired certificates, causing service disruptions and a substantial amount of time and effort spent on resolving these issues.

The interviewees noted how their organizations struggled with common challenges, including:

- **Manual and fragmented certificate management.** Prior to adopting SCM, interviewees' organizations managed their digital certificates manually using spreadsheets or disparate systems. This process was cumbersome and error-prone, often leading to missed renewals and service outages. The lack of centralized control made it difficult to maintain visibility over all certificates, resulting in inefficiencies and increased operational risks.

- **Frequent service outages.** Interviewees noted their organizations experienced frequent service disruptions due to expired certificates. The manual tracking and renewal processes were not reliable, and notifications were often ignored, leading to significant downtime and emergency remediation efforts. This impacted business operations and eroded trust in the organizations' IT infrastructure.

- **High operational costs.** The manual processes for certificate management were labor-intensive and costly. Teams dedicated substantial time to routine tasks like tracking, renewing, and validating certificates. This not only diverted resources from more strategic initiatives but also increased the risk of human error, further driving up operational costs.

- **Lack of automation.** Many interviewees' organizations lacked automation in their certificate management processes. This absence of automated workflows meant that staff had to perform repetitive tasks manually, leading to inefficiencies and increased potential for mistakes. This made it difficult to scale certificate management practices as the number of certificates grew.

- **Inadequate visibility and reporting.** Without a centralized certificate management system, interviewees said their organizations struggled to maintain adequate visibility and reporting capabilities. This made it challenging to track certificate statuses, identify upcoming expirations, and generate reports for compliance and audit purposes. The lack of oversight increased the risk of certificate-related incidents and compliance issues.

- **Resource-intensive internal solutions.** Some interviewees noted their organizations attempted to manage their certificates using internal public key infrastructure (PKI) solutions, which proved to be resource-intensive and difficult to maintain. These internal systems often required significant manual effort to manage, update, and secure, leading to inefficiencies and increasing operational burdens. Additionally, internal PKI solutions lacked the scalability and reliability needed to support growing certificate needs.

> “Managing certificates manually using spreadsheets was extremely time-consuming and prone to errors, leading to frequent service outages.”
>
> DIRECTOR OF SHARED SERVICES, PAYMENT AND TRANSACTIONAL SERVICES

> “The manual processes for certificate management resulted in high operational costs and diverted resources from more strategic initiatives.”
>
> SENIOR TECHNOLOGY MANAGER, FINANCIAL SERVICES/INSURANCE

> “Our organization lacked automation in certificate management, which led to inefficiencies and a higher potential for mistakes.”
>
> PRINCIPAL, GLOBAL CYBERSECURITY SERVICES, FINANCIAL SERVICES/INSURANCE

> “Without a centralized certificate management system, we struggled with inadequate visibility and reporting capabilities, increasing the risk of incidents.”
>
> DIRECTOR OF SHARED SERVICES, PAYMENT AND TRANSACTIONAL SERVICES

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- **Automate the management of digital certificates.** Manual processes were time-consuming and error-prone, leading to missed renewals and service outages. Automated solutions were sought to ensure timely renewals and reduce operational risks.
- **Provide centralized visibility and control.** The interviewees’ organizations struggled with fragmented systems that made it difficult to track certificate statuses and expiration dates. A centralized platform was needed to maintain oversight and streamline certificate management.
- **Integrate with existing systems.** The chosen solution needed to seamlessly integrate with existing IT infrastructure, such as ServiceNow and Azure, to enhance operational efficiency and reduce implementation complexity.
- **Support crypto agility and scalability.** As certificate lifespans shortened and the number of certificates grew, interviewees noted their organizations needed the solution to scale and support agile cryptographic practices to handle frequent renewals and new security standards.
- **Reduce operational costs.** High operational costs were associated with the interviewees’ organizations’ manual certificate management and maintaining

legacy systems. A more cost-effective solution was needed to free up resources and reduce the financial burden on IT departments.

After a request for proposal (RFP) and business case process evaluating multiple vendors, the interviewees' organizations chose SCM and began deployment.

- **Three out of five interviewees' organizations chose to take a phased approach to deployment.** This allowed for smoother integration and less disruption to ongoing operations.
- **SCM was deployed in phases to ensure effectiveness and meet the interviewees' organizations' needs before full-scale implementation.** This phased approach provided the opportunity to address any issues early and adapt the solution to fit specific requirements.

> "Implementing automated certificate management has streamlined our processes, significantly reducing service disruptions and operational costs."
>
> SENIOR TECHNOLOGY MANAGER, FINANCIAL SERVICES/INSURANCE

> "The implementation of automated certificate management has dramatically reduced our operational workload, allowing us to focus on more strategic initiatives."
>
> DIRECTOR OF SHARED SERVICES, PAYMENT AND TRANSACTIONAL 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 five interviewees, 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 enterprise organization is highly complex with approximately 128,000 employees and an annual revenue of $37 billion. The company has approximately four FTEs managing certificates and an average of 100,000 certificates under management.

Deployment characteristics. The composite organization began using the solution in Year 1, following a two-month implementation period. The initial rollout involved a small team of engineers who developed and customized the integration to fit the organization's infrastructure needs. Deployment was phased, starting with critical applications and gradually expanding to cover the entire organization, ensuring minimal disruption and smooth integration. Training sessions and town halls were conducted to familiarize users with the new system, facilitating a seamless transition from the old manual processes to the automated solution provided by Sectigo.

Key Assumptions

$37 billion in revenue

128,000 employees

4 FTEs managing certificates

100,000 average number of certificates

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	Reduced cost of legacy solutions and certificate authority costs	$42,500	$47,813	$53,789	$144,102	$118,563
Btr	Provisioning labor cost reduction	$438,281	$525,938	$631,125	$1,595,344	$1,307,270
Ctr	Renewal labor cost reduction	$251,813	$362,610	$580,189	$1,194,611	$964,503
Dtr	Reduced outage costs	$892,500	$967,500	$1,042,500	$2,902,500	$2,394,196
	Total benefits (risk-adjusted)	$1,625,094	$1,903,860	$2,307,603	$5,836,557	$4,784,532

REDUCED COST OF LEGACY SOLUTIONS AND CERTIFICATE AUTHORITY COSTS

Evidence and data. The interviewees noted that their organizations discontinued the use of legacy solutions, resulting in savings on licensing, IT maintenance, IT solution hosting, and training costs. Furthermore, the interviewees' organizations no longer needed to purchase certificates from other certificate authorities.

- The information security manager at a logistics company told Forrester, "We've definitely saved a ton of time on having to help users ... manage that infrastructure, which we're still doing today, but that's definitely going to go away."
- The senior technology manager at a financial services company explained: "Do you feel like you've eliminated any legacy solutions as a result of [SCM]? Legacy solutions? Yes, definitely."
- The same interviewee discussed how their organization eliminated several provider relationships, including their infrastructure and domain registry provider

and their previous certificate management and security solution provider for identity and encryption.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite experiences an average reduction in legacy solution and certificate authority costs of $50,000 in Year 1, $56,250 in Year 2, and $63,281 in Year 3.

Risks. The value of this benefit can vary across organizations due to the following:

- Use of legacy solutions.
- The licensing, IT maintenance, IT hosting, and training costs.
- Prior certificate authority costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 15%) of $119,000.

> "We eliminated several legacy solutions, which significantly lowered our licensing and maintenance costs, and stopped purchasing certificates from other authorities."
>
> SENIOR TECHNOLOGY MANAGER, FINANCIAL SERVICES/INSURANCE

Reduced Cost Of Legacy Solutions And Certificate Authority Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Reduced cost of legacy solutions and certificate authority costs	Interviews	$50,000	$56,250	$63,281
At	Reduced cost of legacy solutions and certificate authority costs	A1	$50,000	$56,250	$63,281
	Risk adjustment	↓15%			
Atr	Reduced cost of legacy solutions and certificate authority costs (risk-adjusted)		$42,500	$47,813	$53,789
	Three-year total: $144,102		Three-year present value: $118,563		

PROVISIONING LABOR COST REDUCTION

Evidence and data. Provisioning certificates with legacy solutions required more effort compared to Sectigo, while manual provisioning was considerably more time-consuming. Interviewees noted that certificate demands were increasing rapidly, and legacy solutions were unable to scale efficiently to handle a significant portion of the new certificates.

- Interviewees shared that certificate requirements were growing rapidly, and the legacy solutions could not scale to be used to provision a significant percentage of new certificates.
- The senior technology manager at a financial services/insurance company explained: “We’ve streamlined operational costs effectively again. We were using the cert once and applying it to many, so the incidents that we’ve had based on the realization of the effort that we’re putting in, I think just saving the cost in those incidents.”
- The information security manager at a logistics company said: “By streamlining, [business users] have access to the portal now and within 3 to 5 minutes, they can have a cert in their hand. Something that might have taken them quite a long time to go through that request process is now a full self-service platform.”

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

- The legacy solutions handle 30% of certificate provisioning.
- Certificate growth is 20% per year.
- Labor required for certificate provisioning averages 3 minutes per certificate with Sectigo, averages 5 minutes per certificate with the legacy solutions, and averages 120 minutes per certificate when done manually.
- The fully burdened hourly rate for an employee provisioning certificates is $75.

Risks. The value of this benefit can vary across organizations due to the following:

- The ratio of certificates provisioned with legacy solutions vs. manually.
- The annual certificate volume growth.

- The average time required to provision certificates with the legacy solutions and manually.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 15%) of $965,000.

30%

Reduction in labor costs achieved through optimized provisioning processes

> "Automating certificate provisioning has drastically cut down the time we spend on these tasks, allowing our team to focus on higher-priority items."
>
> SENIOR TECHNOLOGY MANAGER, FINANCIAL SERVICES/INSURANCE

Provisioning Labor Cost Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Legacy certificate provisioning count	Interviews	1,500	1,800	2,160
B2	Legacy provisioning time per certificate (minutes)	Interviews	5	5	5
B3	Manual certificate provisioning count	Interviews	3,500	4,200	5,040
B4	Manual provisioning time per certificate (minutes)	Interviews	120	120	120
B5	Sectigo provisioning per certificate (minutes)	Interviews	3	3	3
B6	**Subtotal: Provisioning time reduction due to Sectigo (hours)**	**((B1*B2)+(B3*B4)-(B1+B3)*B5)/60**	**6,875**	**8,250**	**9,900**
B7	Fully burdened hourly rate for an employee provisioning certificates	TEI standard	$75	$75	$75
Bt	Provisioning labor cost reduction	B6*B7	$515,625	$618,750	$742,500
	Risk adjustment	↓15%			
Btr	Provisioning labor cost reduction (risk-adjusted)		$438,281	$525,938	$631,125
	Three-year total: $1,194,611		**Three-year present value: $964,503**		

RENEWAL LABOR COST REDUCTION

Evidence and data. Typically, renewing certificates with legacy solutions required more effort compared to Sectigo, while manual renewals were much more time-consuming. Interviewees observed that the frequency of renewals was increasing each year and was expected to continue rising due to anticipated 90-day renewal requirements.

- Interviewees shared that certificate renewal frequency was getting shorter every year and was expected to continue, partially due to expected 90-day renewal requirements by companies that they work with.

- The principal, global cybersecurity services at a financial services/insurance company told Forrester: “So that’s now part of what I call our 90-day TTL [time to live] effort. … We’re working with Sectigo on automating all of our certificates. … And that automation will then take the human element out of certificate generation as well as the renewal process.”

- The information security manager at a logistics company explained: “Today, you do the same thing with Sectigo. You go to the web server, you export the CSR [certificate signing request], you get assigned by Sectigo, and you import it back into the web server. So the process has not changed. Again, a certificate is a certificate. So the idea here is that we're making it a more well-defined process for users to self-service before you might have to reach out to another team, or you might have to engage the security team and figure out all of that stuff on a call with a bunch of other folks."

- The principal, global cybersecurity services at a financial services/insurance company told Forrester: "We've definitely saved a ton of time on having to help users, having users reaching out and not understanding the process, [and] having users requiring assistance to install all certificates and then [also] managing that infrastructure, which we're still doing today but that's definitely going to go away."
- The information security manager at a logistics company explained: "When I really presented this platform it was to alleviate the problem with certificates expiring. … It could be 50 or 100 or maybe [in the] 20 to 30 range."

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

- The legacy solutions handle 30% of certificate provisioning.
- Certificate growth is 20% per year and the average renewal frequency growth is 25% in Year 1, 30% in Year 2, and 40% in Year 3. These statistics are not presented in the chart because it would complicate the presentation vs. add value.
- Labor required for certificate renewals averages 0.5 minutes per certificate with Sectigo, averages 2 minutes per certificate with the legacy solutions, and averages 45 minutes per certificate when done manually.
- The fully burdened hourly rate for an employee renewing certificates is $75.

Risks. The value of this benefit can vary across organizations due to the following:

- The ratio of certificates renewed with legacy solutions vs. manually.
- The annual certificate volume growth.
- The annual reduction in renewal frequency.

- The average time required to renew certificates with the legacy solutions and manually.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 15%) of $965,000.

25%

Reduction in labor costs achieved through streamlined renewal processes

> "By streamlining our renewal processes, we've seen a significant reduction in labor costs, allowing us to allocate resources more effectively across other critical areas."
>
> SENIOR TECHNOLOGY MANAGER, FINANCIAL SERVICES/INSURANCE

Renewal Labor Cost Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Legacy certificate renewal count	Interviews	2,250	3,240	5,184
C2	Legacy renewal time per certificate (minutes)	Interviews	2	2	2
C3	Manual certificate renewal count	Interviews	5,250	7,560	12,096
C4	Manual renewal time per certificate (minutes)	Interviews	45	45	45
C5	Sectigo renewal per certificate (minutes)	Interviews	0.5	0.5	0.5
C6	**Subtotal: Renewal time reduction due to Sectigo (hours)**	**((C1*C2)+(C3*C4)-(C1+C3)*C5)/60**	**3,950**	**5,688**	**9,101**
C7	Fully burdened hourly rate for an employee renewing certificates	TEI standard	$75	$75	$75
Ct	Renewal labor cost reduction	C6*C7	$296,250	$426,600	$682,575
	Risk adjustment	↓15%			
Ctr	Renewal labor cost reduction (risk-adjusted)		$251,813	$362,610	$580,189
	Three-year total: $1,194,611		**Three-year present value: $964,503**		

REDUCED OUTAGE COSTS

Evidence and data. Interviewees noted the significant impact of automation and centralized control in reducing certificate-related outages and improving operational efficiency.

- According to interviewees, the automation provided by the SCM's integration with Acme reduced the risk of certificate-related outages by ensuring certificates were automatically renewed. This prevented downtime caused by expired certificates and minimized potential revenue, customer satisfaction, and operational losses due to outages.
- Centralizing policy controls over certificate management reduced the risk of incidents at the interviewees' organizations due to improperly configured certificates.
- Broad visibility with proactive reporting and reminders of upcoming certificate expirations significantly reduced the interviewees' organizations' certificate expirations and associated outages.

- Interviewees stated that their teams could respond and resolve certificate-related problems quicker due to SCM’s tracking capabilities.
- The director of shared services at a payment and transactional services company told Forrester, “[This] automation will take the human element out of certificate generation as well as the renewal process.”
- The senior technology manager at a financial services/insurance company told Forrester: “We’ve had some more complicated ones where some things like Azure resources are included and it’s not really a Sectigo problem. It’s a problem that we don’t know where the cert was loaded or how it was loaded and how it was bound to this web application gateway. So those ones take us a little bit longer, but [before SCM], I would say there was at least one [occurrence] a month or maybe more of the certificate expirations occurring.”

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

- The composite experiences one outage per month prior to the Sectigo implementation, growing 10% per year.
- It experiences one outage per year after the Sectigo implementation.
- The overall cost per outage prior to the Sectigo implementation is $100,000.
- There is a 90% reduction in cost to $10,000 per outage after the Sectigo implementation.

Risks. The value of this benefit can vary across organizations due to the following:

- The frequency of outages both prior to the Sectigo implementation and after the implementation.
- The average cost per outage both prior to the Sectigo implementation and after the implementation.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.4 million.

> "We might have 50 to 60 people on a call when a disruptive outage occurs, doing everything from researching, fixing, determining alternatives, etc. All hands-on deck. Reducing them by over 90% is a big deal. Resolution historically would take 4 to 24 hours, frequently around 12 hours. Outages occur much less frequently and when they occur, they are resolved much quicker because there's more information out there to figure out the cause of the outage."
>
> INFORMATION SECURITY MANAGER, LOGISTICS

Reduced Outage Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Outages with legacy and manual solutions	Interviews	12	13	14
D2	Outages with Sectigo	Interviews	1	1	1
D3	Cost per outage with legacy and manual solutions	Interviews	$100,000	$100,000	$100,000
D4	Cost per outage with Sectigo due to faster recovery time	Interviews	$10,000	$10,000	$10,000
Dt	Reduced outage costs	D1*D3-D2*D4	$1,190,000	$1,290,000	$1,390,000
	Risk adjustment	↓25%			
Dtr	Reduced outage costs (risk-adjusted)		$892,500	$967,500	$1,042,500
	Three-year total: $2,902,500		**Three-year present value: $2,394,196**		

UNQUANTIFIED BENEFITS

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

- **Risk reduction and security.** Interviewees noted that Sectigo's management of the signing authority and the elimination of manual certificate management tasks reduced the risk of errors and breaches. Also, the use of Sectigo's managed services reduced the interviewees' organizations' need for physical hardware security modules (HSMs) and the associated risks and costs. An information security manager at a logistics company described: "Security has improved. Architects and the security engineers have mandated the use of certificates for authentication because they are more secure than passwords."

- **Sectigo partnership.** Interviewees spoke highly of Sectigo's proactive and reactive support. A senior manager of cybersecurity at a broadcasting and cable company shared: "We have a great relationship with Sectigo. They have always been very responsive when we have reached out to help with something, ensure we are doing things right, or make an enhancement request."

- **Certificate lifecycle management.** An information security manager at a logistics company noted: "We now manage the entire certificate lifecycle. We follow the request through, make sure that the user gets their cert, and remind them when their expirations are coming up. We handle over 500,000 certificates with four people."

- **Ownership at the source.** An information security manager at a logistics company explained, "Another benefit of [SCM] is that we have been able to get some teams to install, monitor, and renew their own certificates typically via interfaces with other systems. We monitor their activities, and they are replacing certificates on time. That saves us a lot of time. Also, most of the teams handle fixing expired certificates on their own. A nice aside is that we aren't blamed for expired certificates like in the past."

- **Reporting, notifications, and exploring.** Interviewees shared increased confidence in their certificate tracking due to Sectigo's reporting capabilities. The interviewees considered the ability to send expiration notices to certificate owners at scheduled times before expirations a game changer. A senior manager of cybersecurity at a broadcasting and cable company described: “We can now identify self-signed certificates and certificates that are not Sectigo. We tell the owners to stop using those and go to Sectigo.”

> “Using certificates for authentication has significantly improved our security posture, replacing vulnerable password systems and ensuring robust protection.”
>
> Information security manager, logistics

> “Managing over 500,000 certificates with just four people has streamlined our processes and ensured timely renewals and expirations.”
>
> Information security manager, logistics

FLEXIBILITY

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

- **Flexibility in automation.** Automation of certificate management tasks allowed the interviewees’ organizations to handle large-scale certificate issuance and renewals efficiently. An information security manager at a logistics company noted that automation capabilities made their company more agile by enabling quick certificate issuance and renewals, which would have been impossible manually given the volume of certificates managed.

- **Flexibility in scaling.** Scalable solutions provided by Sectigo enabled the interviewees' organizations to expand their usage seamlessly. A senior manager of cybersecurity at a broadcasting and cable company mentioned that the automation and scalability of Sectigo's platform allowed for easy expansion as new business needs arise, ensuring that certificate management could keep pace with organizational growth and technological advancements.
- **Flexibility in integration.** Interviewees noted integration with other systems allowed for smoother operations and reduced the need for multiple management tools. The senior technology manager at a financial services firm highlighted that Sectigo's integration with their existing infrastructure and tools streamlined processes, reduced manual work, and enhanced overall operational efficiency. This capability to integrate seamlessly with various systems ensured that the interviewees' organizations could adapt to new requirements and technologies without significant disruptions.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> "Sectigo has made the company more agile. We can generate thousands of certificates with automation, which would be impossible to manage manually."
>
> SENIOR MANAGER OF CYBERSECURITY, BROADCASTING AND CABLE

> “The automation and scalability of Sectigo’s platform allow for easy expansion as new business needs arise, ensuring that certificate management can keep pace with organizational growth and technological advancements.”
>
> SENIOR MANAGER OF CYBERSECURITY, BROADCASTING AND CABLE

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
Etr	Sectigo implementation costs	$83,600	$0	$0	$0	$83,600	$83,600
Ftr	Implementation services, licensing, and premier services costs	$0	$469,700	$542,300	$577,940	$1,589,940	$1,309,397
	Total costs (risk-adjusted)	$83,600	$469,700	$542,300	$577,940	$1,673,540	$1,392,997

SECTIGO IMPLEMENTATION COSTS

Evidence and data. Interviewees experienced initial setup and implementation costs when integrating Sectigo's certificate management solutions into their systems.

- An information security manager at a logistics company mentioned, "We had to spend considerable time on the initial setup to ensure everything was integrated properly with our existing infrastructure."
- Training costs were incurred as teams needed to familiarize themselves with the new system. The information security manager at the logistics company noted, "We conducted several training sessions and town halls to ensure everyone was up to speed with the new certificate management processes."
- Additional costs included configuring the system to automate certificate renewals and managing the initial deployment.

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

- The composite organization experiences a two-month implementation period for Sectigo's certificate management solutions.

- Deployment is phased. It starts with critical applications and gradually expands to cover the entire organization, ensuring minimal disruption and smooth integration.
- Initial internal costs to the customer was $20,000.
- Professional services implementation costs charged by Sectigo was $56,000.

Risks. The value of this cost can vary across organizations due to the following:

- Variability in the complexity of existing infrastructure can lead to longer implementation times and higher initial setup costs.
- The need for extensive customization and integration with other systems can increase costs beyond initial estimates.
- Unanticipated training requirements and additional support needed for users to become proficient with the new system can raise overall implementation costs.
- Potential delays in the deployment phase can result in increased costs due to extended project timelines.

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 $84,000.

> "The implementation process required us to coordinate with multiple departments to ensure seamless integration, which took about two months."
>
> SENIOR MANAGER OF CYBERSECURITY, BROADCASTING AND CABLE

Sectigo Implementation Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Implementation costs	Composite	$20,000			
E2	Implementation costs for Sectigo professional services	Composite	$56,000			
Et	Sectigo implementation costs	E1+E2	$76,000	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Sectigo implementation costs (risk-adjusted)		$83,600	$0	$0	$0
	Three-year total: $83,600		**Three-year present value: $83,600**			

IMPLEMENTATION SERVICES, LICENSING, AND PREMIER SERVICES COSTS

Evidence and data. Interviewees experienced initial setup and ongoing costs for implementation services, licensing, and premier services when integrating Sectigo's certificate management solutions. The setup involved coordinating with multiple departments and took approximately two months with additional costs for training, automating certificate renewals, and managing the deployment. The financial model indicated initial and Year 1 costs for implementation services, licensing, and premier services.

- An information security manager at a logistics company mentioned, "We had to spend time and resources on the initial setup to ensure everything was integrated properly with our existing infrastructure."
- Interviewees noted training costs were incurred to familiarize teams with the new system. The information security manager at the logistics company noted, "We conducted several training sessions and town halls to ensure everyone was up to speed with the new certificate management processes."
- Additional costs included configuring the system to automate certificate renewals and managing the initial deployment.

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

- The Sectigo licenses for the composite organization are estimated to be $378,000 in Year 1, $444,000 in Year 2, and $476,400 in Year 3.
- The premier services for the composite organization are estimated to be $49,000 annually.

Risks. The value of this cost can vary across organizations due to:

- Variability in the complexity of existing infrastructure can lead to longer implementation times and higher initial setup costs.
- The need for extensive customization and integration with other systems can increase costs beyond initial estimates.
- Unanticipated training requirements and additional support needed for users to become proficient with the new system can raise overall implementation costs.

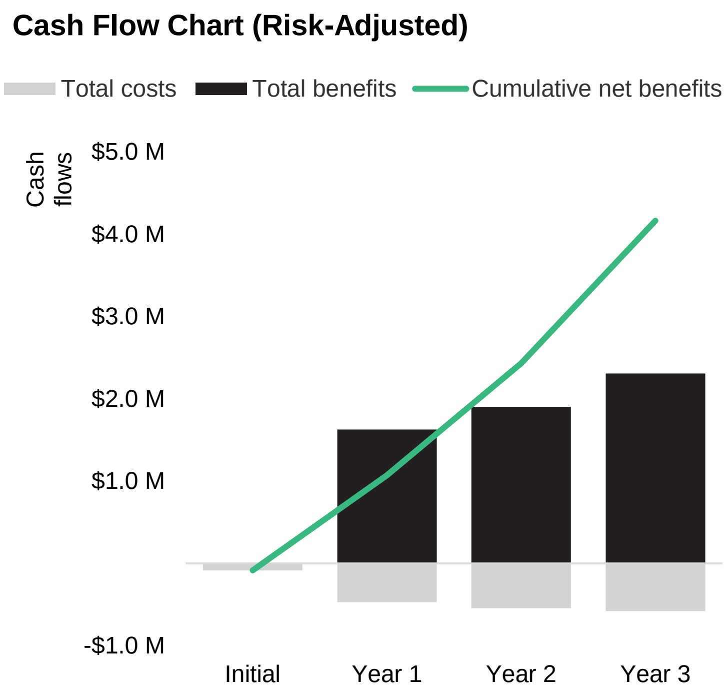
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.3 million.

Implementation Services, Licensing, And Premier Services Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Sectigo licenses	Composite		$378,000	$444,000	$476,400
F2	Premier services	Composite		$49,000	$49,000	$49,000
Ft	Implementation services, licensing, and premier services costs	F1+F2	$0	$427,000	$493,000	$525,400
	Risk adjustment	↑10%				
Ftr	Implementation services, licensing, and premier services costs (risk-adjusted)		$0	$469,700	$542,300	$577,940
	Three-year total: $1,589,940		**Three-year present value: $1,309,397**			

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 Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($83,600)	($469,700)	($542,300)	($577,940)	($1,673,540)	($1,392,997)
Total benefits	$0	$1,625,094	$1,903,860	$2,307,603	$5,836,557	$4,784,532
Net benefits	($83,600)	$1,155,394	$1,361,560	$1,729,663	$4,163,017	$3,391,535
ROI						243%
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 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.

FORRESTER®