FORRESTER®

The Total Economic Impact™ Of Microsoft Azure Resilience Guidance

Cost Savings And Business Benefits Enabled By Microsoft Azure Resilience Guidance

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY MICROSOFT, JUNE 2024

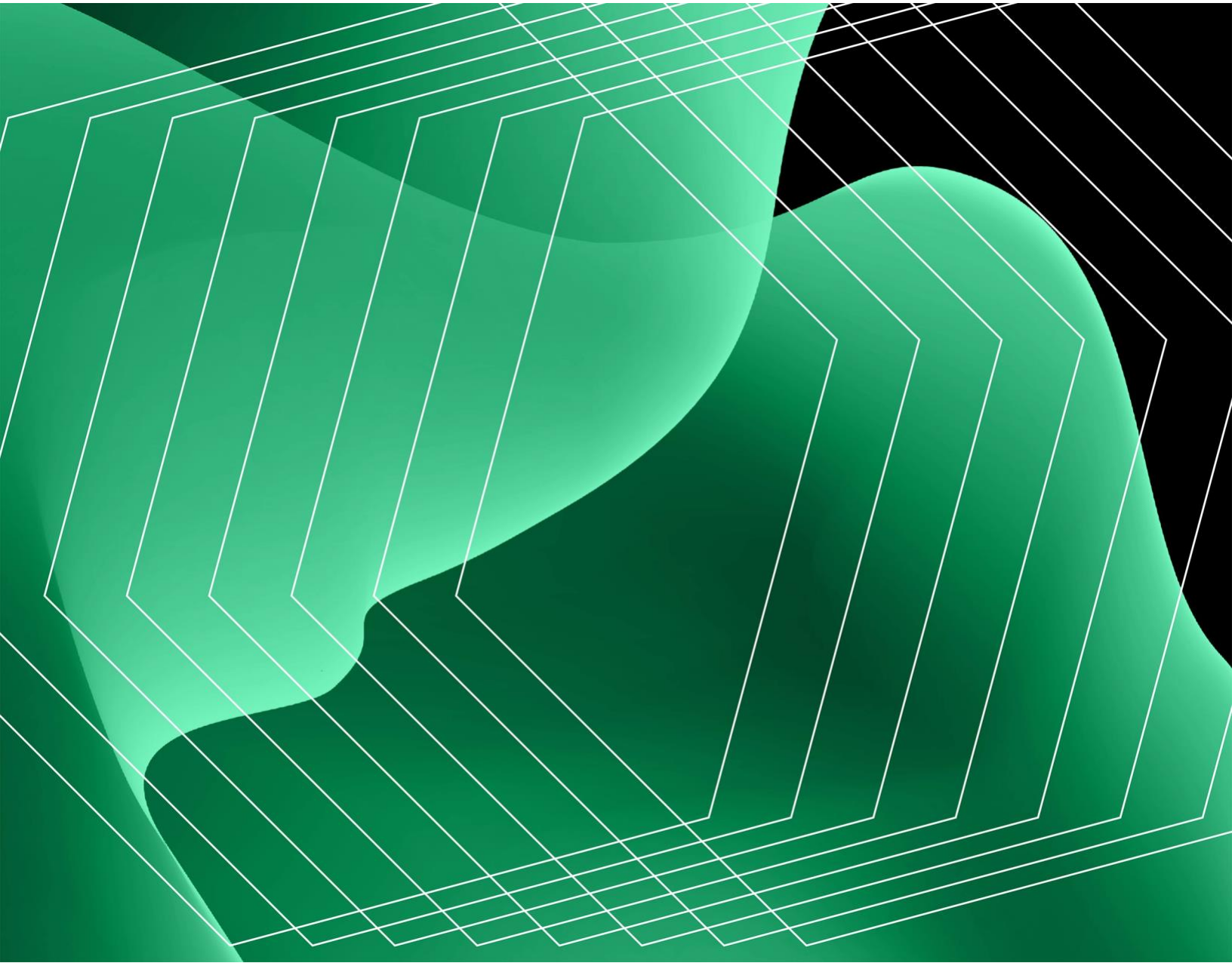


Table Of Contents

Consulting Team:

Nikoletta Stergiou

Carmen Serradilla Ortiz

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.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Even though the cloud-native ecosystem is continuously changing, developers can establish redundancy in their designs to enable horizontal scalability while ensuring there is never a single point of failure.[1] Through Microsoft Azure resilience guidance, Microsoft aims to address the modernization of critical workloads on Azure by offering a set of quality-driven tenets, architectural decision points, and review tools intended to help solution architects build a technical foundation for their workloads.

Microsoft Azure resilience guidance provides solution architects with guidance to build secure, reliable, and high performing applications through tools including the Microsoft Cloud Adoption Framework (CAF), Azure Well-Architected Framework (WAF) and Azure Advisor. These are all based on five tenets: cost optimization, security, reliability, operational excellence, and performance efficiency. Architecture teams can use these review tools to assess their readiness in deploying workloads to production and ensuring resilience.

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by using the Microsoft Azure resilience guidance.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of improving resilience of their workloads by following the principles of the Microsoft Azure resilience guidance on their organizations.

To understand the benefits, costs, and risks associated with this investment, Forrester interviewed nine representatives with experience going through the Microsoft Azure resilience guidance. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. This organization is defined as a global, $20 billion organization with 50,000 employees and has 500 critical workloads.

Return on investment (ROI)
18%

Net present value
$789K

Interviewees said that prior to their utilization of Microsoft Azure resilience guidance tools — including the Azure Well-Architected Framework (WAF) and Azure Advisor — their organizations were migrating from on-premises to public cloud. Rather than choosing migration techniques for each workload, these organizations opted for a lift-and-shift approach. Without the proper training and expertise in the principles of the Microsoft Azure resilience guidance, architects and their teams struggled with migration. These limitations led to failures in resilience and reliability, suboptimal workload efficiency, and outages related to app and platform performance.

After implementing the recommendations from Microsoft Azure resilience guidance, the interviewees could create a more resilient cloud environment and improve their methods in architecting their critical workloads on Azure. Key results from the investment include improved resilience and performance, workload optimization, improved operational efficiency, reduction in planned downtime, and improved security posture.

KEY FINDINGS

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

- **Improved resilience and performance, avoiding revenue loss from resilience issues by 15%.** The composite organization experiences resilience issues on their critical workload prior to reviewing Azure Guidance Offering tools, such as the WAF Review and Advisor. On average, critical workloads contribute 0.15% to revenue on an annual basis. By the end of Year 3, the composite avoids 15% of revenue loss through improved resilience. Over three years, this improvement is valued at more than $650,000 to the composite organization.
- **Optimized workloads by 15% with increased scalability via re-architecture.** The composite organization incrementally migrates its critical workloads to Azure. On average, each workload costs $156,000 without using the principles of the Microsoft Azure resilience guidance. With the implemented recommendations from these tools, the organization improves scalability through re-architecture

and improves workload optimization by 15%. Over three years, workload optimization is valued at around $2.4 million to the composite organization.

- **Increased operational efficiency by 20%.** The composite organization has 25 dedicated Azure system administrators. Using recommendations from Microsoft Azure resilience guidance improves system administrator operational efficiency by 20% by Year 3. Over the course of three years, improved operational efficiency is worth $555,000 to the composite organization.
- **Reduced planned downtime by 30%.** Prior to the organization's utilization of Microsoft Azure resilience guidance, the composite has an average of 100 hours of planned downtime per year. After implementing the recommendations, there is a 30% reduction in planned downtime by Year 3. Over the course of three years, the reduction in planned downtime is worth $1.2 million to the composite organization.
- **Improved security posture against external attacks by 20%.** While the initial migration to Azure improves the composite organization's overall security posture by reducing the percentage of external attacks, following the Microsoft Azure resilience guidance recommendations further reduces the risk against external attacks by 20%. Over the course of three years, the improvement in security posture is worth more than $321,000 to the composite organization.

Percentage of avoided revenue loss due to resilience issues after implementing Microsoft Azure resilience guidance recommendations

15%

> “The value that the Well-Architected Framework brings is that it improved the overall productivity of our development and customer experience by having more uptime and better performance, and our ability to provide the best services as compared to our competitors and maintain that competitive advantage.”
>
> **VICE PRESIDENT OF CLOUD ARCHITECTURE, FINANCIAL SERVICES**

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

- **Microsoft partnership.** The composite organization’s partnership with Microsoft enables their access to technology expertise, scalable and secure infrastructure, a broad portfolio of solutions, a supportive ecosystem, integration capabilities, innovation opportunities, and trust and reliability. With extensive support resources, a strong commitment to security and compliance, and a focus on innovation, partnering with Microsoft empowers the composite organization’s ability to stay ahead of the curve, foster growth, and achieve their business objectives.
- **Improved customer satisfaction and retention.** The improvement in resilience and performance enhanced customer satisfaction and therefore retention. Consistent, uninterrupted access to services and applications builds trust and confidence in the brand. It also encourages higher customer satisfaction as business targets could be met with minimal downtime on business operations.
- **Avoided penalty fees.** Following the Microsoft Azure resilience guidance recommendations improves service-level agreements (SLAs). The composite organization avoids penalty fees by setting clear performance metrics, raising performance standards, implementing monitoring and reporting processes, defining remediation procedures, and introducing financial incentives. Clear definitions and targets in SLAs aligns expectations between service providers

and customers, while higher performance standards motivates service providers to maintain a higher level of service quality.

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

- **Initial re-architecting costs on Azure.** The initial re-architecting of critical workloads on Azure requires 20 architects. Over the course of six months, these architects spend 50% of their time re-architecting on Azure.
- **Ongoing management costs of critical workloads on Azure.** Twenty-five system administrators dedicate 25% of their time toward the ongoing management of critical workloads by following the Microsoft Azure resilience guidance. They spend 10% of their time on any new practices and principles that are updated in the framework.

The representative interviews and financial analysis found that a composite organization experiences benefits of $5.1 million over three years versus costs of $4.3 million, adding up to a net present value (NPV) of $789,000 and an ROI of 18%.

ROI

18%

BENEFITS PV

$5.1M

NPV

$789K

PAYBACK

27 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 Microsoft Azure resilience guidance.

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 Microsoft Azure resilience guidance can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Microsoft 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 Microsoft Azure resilience guidance.

Microsoft 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.

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

1. **Due Dilligence**
   Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft Azure resilience guidance.
2. **Interviews**
   Interviewed nine representatives at organizations using Azure resilience guidance 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 Microsoft Azure Resilience Guidance Customer Journey

Drivers leading to the Microsoft Azure resilience guidance

Interviews				
Role	**Industry**	**Region**	**Annual Revenue, Number Of Employees**	**Percentage Of Critical Workloads On Azure**
Vice president, platforms, cloud and object storage service (OSS)	Telecommunications	Canada	$13.5 billion, 22,000 employees	Not applicable
Vice president of cloud architecture	Financial services	HQ in the US, global operations	$12.1 billion, 23,000	85%
Director of software engineering	Communications and IT	HQ in the US, global operations	$57 billion, 84,900 employees	25%
Senior director of IT and CIO	Healthcare	HQ in the US, global operations	$7.7 billion, 49,000 employees	30%
Vice president of technology	Pharmaceuticals	US	$40 billion, 120,000	80%
Cloud security principal	Insurance	US	$2.3 billion, 13,000 employees	50%
CTO	Retail	Australia and New Zealand	$25.1 billion, 120,000	80%
Vice president and CISO	Financial services	HQ in the US, global operations	$1.3 billion, 17,000 employees	45%
Lead voice network designer	Telecommunications	HQ in the UK, global operations	$26.1 billion, 98,800 employees	Not applicable

KEY CHALLENGES

Prior to going through the Microsoft Azure resilience guidance, interviewees highlighted key challenges in managing workloads. These included reliability and resilience issues due to communication gaps and non-optimal practices, difficulties in optimizing workload efficiency during cloud transitions, skill gaps on their team and the need to enhance their team's capabilities on the Azure platform, and outages related to app or platform performance due to poorly architected workloads. These challenges led to downtime, data loss, performance issues, scalability limitations, security vulnerabilities, and customer dissatisfaction.

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

- **Outages related to app or platform performance.** Interviewees highlighted that poorly-architected workloads resulted in challenges related to outages and performance issues with applications or platforms. Scalability issues arose when the architecture failed to handle increased user demand or traffic spikes. Additionally, inefficient usage of resources led to wasted resources or performance bottlenecks. The vice president of cloud architecture at a financial services organization described a situation where a critical workload hosted on-premises crashed and noted the level of effort required to remediating this: "During a peak time, the application crashed because of the high traffic and our infrastructure could not support that high volume of traffic. Because of this, we migrated to the backup server by default, but the backup server — not being infrastructurally capable to manage that high volume as well — also started showing performance issues. So, people were not able to access the application or it was crashing."

  The CTO at a retail organization shared the impact that performance issues can have on an organization: "It's not always [about] money, but what it does do is brand damage. If you only have one [performance issue], customers are usually forgiving, especially if there's a notice. However, if that's happening regularly, that's a real problem."
- **Reliability and resilience issues due to communication gaps and non-optimal practices.** Interviewees described how non-optimal practices and communication gaps in their prior environments significantly impacted the reliability and resilience of their organization's workloads. Challenges included a lack of disaster recovery planning, inadequate monitoring and proactive maintenance, insufficient communication and collaboration among teams, poor change management practices, and inefficient incident response and resolution. Failure to address these challenges resulted in downtime, data loss, performance issues, and delayed problem resolution. The senior director of IT and CIO at a healthcare organization described a lack of communication across their infrastructure environment which led to these issues, noting, "From a system administrator standpoint, being able to administer different types of enterprise

workloads in different siloed environments always posed a lot of challenges."

The vice president of technology at a pharmaceutical organization further highlighted the results of their initial attempts to move workloads from their on-premises environment to Azure, noting: "We had gone through this sort of notion of doing sort of a self-service model, and there were some issues from a governance perspective where it was a little bit [disorganized]. We needed to put better governance controls so that we didn't have some of the security risks like for example, having the wrong people accessing the wrong data."

- **Challenges in optimizing workload efficiency during cloud transition.** Interviewees described how their organizations performed a lift-and-shift of workloads from on-premises to the cloud, in which they encountered challenges such as compatibility issues where applications and dependencies could not seamlessly transition to the new environment. This led to performance and cost optimization concerns as the cloud infrastructure might require different configuration and resource allocation to ensure optimal operation and cost efficiency. The vice president and CISO at a financial services organization described this process at their organization, commenting, "Similar with security-related settings as well, a lot of times we'd bring something over and we either brought the settings from an on-premises version which was not optimal from a security perspective in the cloud, or we just took the default settings from the workload in the cloud instead of actually understanding what they should be and setting them correctly."

  The senior director of IT and CIO at a healthcare organization also highlighted the challenge in scaling a workload during the cloud transition and the impact on scalability of workloads, noting, "Our storage costs kept going up because in healthcare, the one thing that's always been true is that our data footprint kept growing. We ran into a lot of capacity issues."

  Furthermore, the vice president of cloud architecture at a financial services organization described the need to properly architect workloads onto Azure: "The most important thing is to make sure we understand that on-premises infrastructure is not exactly what you want to replicate into Azure. You will need to

re-architect your current workloads and making sure that it fits to the needs of the Azure framework."

- **Skill gaps and the need to enhance team capabilities.** Interviewees highlighted that teams responsible for architecting workloads on the cloud may encounter skill gaps in various areas. These skill gaps included a lack of expertise in cloud architecture, proficiency in Azure, knowledge of security and compliance practices in the cloud, automation skills, performance optimization techniques, and cost optimization and management. Interviewees noted that security was a significant concern when migrating to the cloud, and skill gaps in this area can be detrimental to their organization's overall security posture. Cloud security requires a deep understanding of the shared responsibility model, identity and access management, data encryption, network security, and compliance requirements. Interviewees noted some instances where they overlooked critical security considerations or misconfigured access controls, that left their cloud infrastructure vulnerable to cyber threats.

  The vice president of technology at a pharmaceutical company shared a security incident example that could have been prevented with the right expertise: "One of our developers had put credentials on a [developer platform] environment, and that credential got leaked. We realized that we didn't have the right sort of alerting mechanisms in place, so a bad actor was found using it to do some level of crypto mining. This cost us about $250,000."

  The vice president and CISO at a financial services organization further commented on the skill gaps in their organization as it related to new cloud environments: "I can say, on the security side, this was a relatively new environment for my security team. So, we were still getting up to speed on essentially securing cloud-based workloads and could use all the help in terms of ensuring that we were doing everything properly."

> “We had an on-premises solution in our prior environment and faced several challenges. One challenge is that we are not into the technology business, so we always had a lack of technical expertise to manage the solution on-premises. Secondly, infrastructure management and overhead were difficult to manage. Thirdly, the reliability and scalability. Our infrastructure was not as reliable as Azure services are.”
>
> VICE PRESIDENT OF CLOUD ARCHITECTURE, FINANCIAL SERVICES

INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- **Maintain business continuity.** Organizations want to make critical apps more resilient and secure to ensure uninterrupted operations and maintain business continuity.
- **Improve customer trust and reputation.** Enhancing the resilience and security of critical apps can build customer trust and protect the organization's reputation.
- **Offer regulatory compliance.** Organizations aim to meet regulatory requirements for data protection and application security.
- **Mitigate financial losses.** Improving the resilience and security of critical apps can minimize the risk of financial losses due to downtime or security breaches.
- **Offer future scalability.** Making critical applications more resilient and secure prepares organizations for future growth and scalability.

> “With regards to points of reliability, it’s really been the resilience of workloads and looking at things related to monitor disaster recovery and change management within the platform that has been in my opinion, really rock solid.”
>
> SENIOR IT DIRECTOR AND CIO, HEALTHCARE

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 nine 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, $20 billion organization has 50,000 employees and 500 critical workloads. There are 25 system administrators as well as 20 architects.

Description of deployment characteristics. The composite is on a migration journey on migrating critical workloads from an on-premises environment to Azure. The composite moves 5% of critical workloads to Azure in Year 1, 10% in Year 2, and 15% in Year 3. In the initial architecting phases, the composite does not follow Microsoft Azure resilience guidance recommendations and encounters resilience, security, and cost optimization issues.

KEY ASSUMPTIONS

$20 billion in annual revenue

50,000 employees

500 critical workloads

15% of critical workloads on Azure by Year 3

25 system administrator FTEs

20 architect FTEs

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 resilience and performance	$135,000	$270,000	$405,000	$810,000	$650,150
Btr	Optimized workloads	$497,250	$994,500	$1,491,750	$2,983,500	$2,394,720
Ctr	Improved operational efficiency	$151,875	$227,813	$303,750	$683,438	$554,555
Dtr	Reduced planned downtime	$240,000	$480,000	$720,000	$1,440,000	$1,155,823
Etr	Improved security posture	$129,167	$129,167	$129,167	$387,502	$321,220
	Total benefits (risk-adjusted)	$1,153,292	$2,101,480	$3,049,667	$6,304,439	$5,076,468

IMPROVED RESILIENCE AND PERFORMANCE

Evidence and data. Interviewees highlighted improvements in resilience and performance achieved through the implementation of Microsoft Azure resilience guidance recommendations on architecture design and optimization. Through building reliable and fault-tolerant systems, optimizing performance efficiency, and implementing cost optimization strategies, the framework helped interviewees address security considerations to protect their critical workloads. By following Microsoft Azure resilience guidance's principles and recommendations, the interviewees noted they could design, optimize, and operate their Azure workloads in a way that enhanced resilience and improved performance.

- The senior director of IT and CIO at a healthcare organization highlighted the impact that the recommendations had on their critical workload uptime: “Uptime has improved because we’re not having to take down production to then re-provision new hardware to be able to do that. We are enabled to flex up or flex down as needed in the cloud environment.”

- The vice president of technology at a pharmaceutical organization cited a 10% to 15% improvement in performance as a result of re-architecting a workload with Microsoft Azure resilience guidance: “There was one specific sort of API call, if I recall correctly, that was sort of taking longer than expected to return data and there were some specific firewall rules that we had put in place that was slowing down the pipe between that app and the underlying database that it was trying to access. I would say that that pipe needed to be sort of opened up a little bit without compromising security.”
- The cloud security principal at an insurance organization described a specific use case in which costs increase significantly, is when critical workloads associated with claims are down: “When we can't provide claims and everything starts to go into an offline mode, it starts to drive up cost because if the system is unavailable and somebody needs to check if a provider needs to get a quote or somebody's eligibility, they start calling our call centers, and then the call centers started going up. Then you're starting to bring on additional resources to handle phone calls and the manpower rates go up. We continue the business, but it becomes very expensive from a recovery standpoint when you're down.”
- The director, software engineer at a communications and IT organization discussed the improvement in uptime of workloads on Azure as a result of implementing the Microsoft Azure resilience guidance recommendations: “Azure workloads have the lowest percentage of failure in our organization compared to other cloud platforms we use. On our top app, we have 100 users per hour, and 98% to 99% of those are successful, sustained, and delivered.”

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

- Critical workloads contribute 0.15% of revenue toward the $20 billion annual revenue.
- After implementing the Azure Well-Architected Review recommendations, the composite avoids 5% of revenue loss due to resilience issues in Year 1, 10% in Year 2, and 15% in Year 3.
- There is a 10% profit margin.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Annual revenue.
- The percentage of average revenue generated by critical workloads.
- The profit margin.

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 $650,000.

Avoided revenue loss due to resilience issues after implementing Microsoft Azure resilience guidance recommendations by Year 3

15%

"We actually were able to change our SLAs to five-nines from four-nines by migrating to Azure and following Microsoft Azure resilience guidance. We improved the performance of some of our customer-facing applications by as much as 10%. We're able to essentially get faster performance of the app using the same resources."

VICE PRESIDENT AND CISO, FINANCIAL SERVICES

Improved Resilience And Performance					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Annual revenue	Composite	$20,000,000,000	$20,000,000,000	$20,000,000,000
A2	Percentage of average revenue generated by critical workloads	Composite	0.15%	0.15%	0.15%
A3	Average revenue generated by critical workloads per year	A1*A2	$30,000,000	$30,000,000	$30,000,000
A4	Percentage of avoided revenue loss due to resilience issues after implementing Microsoft Azure resilience guidance recommendations	Interviews	5%	10%	15%
A5	Profit margin	TEI standard	10%	10%	10%
At	Improved resilience and performance	A3*A4*A5	$150,000	$300,000	$450,000
	Risk adjustment	↓10%			
Atr	Improved resilience and performance (risk-adjusted)		$135,000	$270,000	$405,000
	Three-year total: $810,000			**Three-year present value: $650,150**	

OPTIMIZED WORKLOADS

Evidence and data. Interviewees described how applying best practices and principles to design and operate workloads on Azure efficiently with Microsoft Azure resilience guidance equipped them to optimize their workloads by leveraging Azure's scalability, elasticity, and managed services. Additionally, the framework encouraged the use of monitoring and alerting to identify performance bottlenecks and proactively address them to ensure resilience was maintained.

- The CTO of a retail organization described the impact of understanding workload design principles on reducing the cost of running more resilient workloads: “Resilience has a very direct commercial impact. When you think about the design principles that you get from reliability, they exist at a number of levels. So clearly you got to understand the business service, and the criticality because there is a cost associated with building in that reliability.”
- The CTO of a retail organization described how their team did not properly construct applications to take advantage of landing zones prior to the Microsoft Azure resilience guidance, such as setting up Kubernetes Services so that they will seamlessly fail over and spin up additional clusters. The CTO commented:

> "What we found was, the way my team had architected the solution by assuming that every zone and region was going to have 100% availability in order for it to assume that its services would be 100% available. With the Microsoft Azure resilience guidance, we were given recommendations on how to construct our applications to take advantage of landing zones."

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

- There are 500 critical workloads. Of which, the composite migrates 5% to Azure in Year 1, 10% by Year 2, and 15% by Year 3.
- The average cost per workload on Azure prior to implementing the framework principles is $156,000.
- With the implementation of recommendations from the Microsoft Azure resilience guidance, the cost to run workloads is reduced by 15%.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The number of critical workloads on Azure.
- The average cost per workload on Azure.
- The type of resilience recommendations implemented to achieve the resilience needed to run and maintain critical workloads.

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 $2.4 million.

Reduction in cost to run workloads based on Microsoft Azure resilience guidance recommendations

15%

> "We were so reactive when it came to data storage. Now we're proactive. From a cost optimization standpoint, having those types of insights and models that can provide, "hey, this is how things are looking as your data footprint has grown, this is how you're able to right size what those types of situations are," to be able to optimize costs while ensuring that it works from a performance and reliability standard."
>
> **SENIOR DIRECTOR OF IT AND CIO, HEALTHCARE**

Optimized Workloads					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Total critical workloads	Composite	500	500	500
B2	Percentage of critical workloads on Azure	Composite	5%	10%	15%
B3	Critical workloads on Azure	B1*B2	25	50	75
B4	Average cost per workload in prior environment	Composite	$156,000	$156,000	$156,000
B5	Percentage reduction in cost to run workloads based on Microsoft Azure resilience guidance recommendations	Interviews	15%	15%	15%
Bt	Optimized workloads	B3*B4*B5	$585,000	$1,170,000	$1,755,000
	Risk adjustment	↓15%			
Btr	Optimized workloads (risk-adjusted)		$497,250	$994,500	$1,491,750
	Three-year total: $2,983,500			**Three-year present value: $2,394,720**	

IMPROVED OPERATIONAL EFFICIENCY

Evidence and data. Interviewees noted how the Microsoft Azure resilience guidance provided a standardized approach, comprehensive guidance, and risk mitigation strategies to create more resilient workloads on Azure. Their teams created a proactive and continuous improvement mindset, allowing them to identify and address risks in workload architecture early on, optimize their architectures, and stay up to date with evolving cloud practices. Teams were better equipped for collaboration and knowledge sharing as they took in continuous feedback and recommendations from Microsoft Azure resilience guidance tools. By following the frameworks and recommendations, interviewees highlighted how their FTEs could streamline decision-making and drive greater efficiency in their cloud architecture processes.

- The director of software engineering at a communications and IT organization described avoided talent costs in creating resilient workloads as a result of insights provided through Microsoft Azure resilience guidance: “I’m not going to have to go and hire more expensive consultation to retrofit something because it didn’t pass 11th hour. And my long-term plan is to showcase. When we stood up these other cloud platforms, Azure was able to meet the demand and help us grow into the market.”
- The senior director of IT and CIO at a healthcare organization described the impact of Microsoft Azure resilience guidance on reskilling and upskilling his team: “Reskilling and upskilling those folks, shifting now from being in an on-prem environment and supporting a cloud hosted environment Azure, it’s not a very hard uplift to do that. It’s very intuitive and Microsoft does a very good job at setting up what that migration process looks like for what we’ll call knowledge workers and those that have an understanding of data center operations, storage operations, and things like that.”
- The director of software engineering at a communications and IT organization discussed the continuous training of their team enabling them to be updated on resilient workloads. They noted, “We take those Microsoft Azure resilience guidance suggestions hourly, and we’re feeding that back to our team to make sure that we don’t have any issues.”

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

- There are 25 system administrators dedicated to Azure.
- There is a 10% improvement in system administrator operational efficiency as a result of the Microsoft Azure resilience guidance recommendations in Year 1, 15% improvement in Year 2, and 20% improvement in Year 3.
- The fully-burdened annual salary of a system administrator is $135,000.
- There is a 50% productivity recapture to account for improved work-life balance.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The number of system administrators.
- The average fully-burdened annual salary of a system administrator.

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 $555,000.

Improvement in system administrator operational efficiency as a result of Microsoft Azure resilience guidance recommendations by Year 3

20%

> “From a change management standpoint, we’ve been really able to minimize the disruption in business because of Microsoft Azure resilience guidance.”
>
> SENIOR DIRECTOR OF IT AND CIO, HEALTHCARE

Improved Operational Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	System administrators dedicated to Azure	Composite	25	25	25
C2	Percentage improvement in system administrator operational efficiency as a result of Microsoft Azure resilience guidance recommendations	Interviews	10%	15%	20%
C3	Average system administrator fully-burdened annual salary	Composite	$135,000	$135,000	$135,000
C4	Productivity recapture	TEI standard	50%	50%	50%
Ct	Improved operational efficiency	C1*C2*C3*C4	$168,750	$253,125	$337,500
	Risk adjustment	↓10%			
Ctr	Improved operational efficiency (risk-adjusted)		$151,875	$227,813	$303,750
	Three-year total: $683,438			**Three-year present value: $554,555**	

REDUCED PLANNED DOWNTIME

Evidence and data. Interviewees highlighted that they are better equipped with Microsoft Azure resilience guidance on managing planned downtime effectively in Azure as it encourages the design and implementation of highly available architectures. It emphasizes the use of redundancy, fault tolerance, and load balancing to ensure that workloads can remain operational even during planned downtime. By implementing

strategies such as multiregion deployment or active-active configurations, teams can minimize the impact of planned downtime on end users.

Furthermore, interviewees noted that establishing maintenance windows during periods of low user activity minimized disruptions. Thorough testing and rollback strategies ensured smooth maintenance processes and quick recovery from unforeseen issues. By following the Microsoft Azure resilience guidance's recommendations, teams can effectively manage planned downtime, maintain high availability, and enhance overall system reliability.

- The cloud security principal at a healthcare organization described disaster recovery drills while maintaining production: “We run disaster recovery drills twice a year. It’s a good several-week-long exercise where we're looking at all the mission critical applications that we go through. We keep production running of course, but we're bringing up our backup environments and a lot of those involve Azure. In fact, one of our goals is to move more towards Azure to make it easier for us to use those facilities rather than, you know, trying to recover the on-prem environment.”

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

- There is an average of 100 planned downtime hours per year prior to the framework. The average hourly cost of downtime is $30,000.
- The recommendations from the Microsoft Azure resilience guidance reduces planned downtime by 10% in Year 1, 20% in Year 2, and 30% in Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The number of planned downtime hours per year.
- The hourly cost of planned downtime.

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 $1.2 million.

Reduction in downtime as a result of Microsoft Azure resilience guidance recommendations

30%

"That's how we've been able to manage our cloud-hosted environments versus on-prem data and storage environments, where you have to do patch management, system refreshes, add additional hardware, and things like that. Reduction in planned downtime really is the best way we have been able to measure that."

SENIOR DIRECTOR OF IT AND CIO, HEALTHCARE

Reduced Planned Downtime					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Average planned downtime hours per year in prior environment	Composite	100	100	100
D2	Percentage reduction in planned downtime as a result of Microsoft Azure resilience guidance recommendations	Interviews	10%	20%	30%
D3	Hourly cost of planned downtime	Composite	$30,000	$30,000	$30,000
Dt	Reduced planned downtime	D1*D2*D3	$300,000	$600,000	$900,000
	Risk adjustment	↓20%			
Dtr	Reduced planned downtime (risk-adjusted)		$240,000	$480,000	$720,000
	Three-year total: $1,440,000			**Three-year present value: $1,155,823**	

IMPROVED SECURITY POSTURE

Evidence and data. Interviewees highlighted how they used the Microsoft Azure resilience guidance to improve their organization's security posture. The Microsoft Azure resilience guidance emphasizes the importance of implementing security measures in cloud architectures, including distributed denial of service (DDoS), malware attacks, zero-day exploits, social engineering attacks, and more. By following the framework's recommendations, interviewees noted their organizations were enabled to proactively identify and address security risks, automate security controls, ensure secure data management, and foster a culture of security awareness to ensure resilience of their workloads.

- The vice president and CISO at a financial services organization discussed how they measure an improved security posture as it relates to resilience: "One of the reasons behind that would be that the availability is an important component of resiliency. If the apps are down, we end up suffering financially from that, but on the security side, we essentially measure annual loss expectancy from a data breach, for instance, and that annual loss expectancy — if we secure our environment, it goes down. Meaning, we would expect to pay less from incurring a data breach. All that goes into the calculation for us, is what is that reduction in annual loss expectancy from securing our workloads."

- The vice president of cloud architecture at a financial services organization cited a reduction in vulnerabilities after implementing Microsoft Azure resilience guidance recommendations: “We have this overall security incidents like malware infections or even unauthorized access attempts. The attempts have increased, but the level of security has increased for us as well.”
- The lead voice network designer at a telecommunications organization shared an example of a Microsoft Azure resilience guidance recommendation related to the vulnerabilities of a workload: “There’s a clear recommendation to protect the platform as a service or software as a service from having it open to the public. The Microsoft Azure resilience guidance recommendation was to lock it down to certain networks that need to communicate with that service. That was black-and-white clear that had to be done immediately because it is a security risk.”

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

- According to Forrester Research, there is an 89% likelihood of experiencing one or more breaches per year for an organization of 50,000 employees. The mean cumulative cost of breaches is $6,158,000, which includes average remediation and reporting labor costs, average costs of response and notification, fines, damages, compliance costs, customer compensation, average lost business revenues and additional costs to acquire customers, and end-user downtime as it relates to a security breach across the organization. Furthermore, the risk of a breach originating from external attacks is 49.1%.[3]
- The migration of critical workloads to Azure helps to address 30% of these attacks.
- With the implementation of the Microsoft Azure resilience guidance recommendations, there is a 20% reduction in the risk of breaches from external attacks.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The size of the organization including revenue and number of employees.

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 $321,000.

Reduced risk of breaches from external attacks with Microsoft Azure resilience guidance recommendations

20%

"We did everything to make a workload more resilient and secure with Microsoft Azure resilience guidance. Resilience and security is the topmost priority for us."

VICE PRESIDENT OF CLOUD ARCHITECTURE, FINANCIAL SERVICES

Improved Security Posture					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Likelihood of experiencing at least one breach per year	Forrester research	89%	89%	89%
E2	Mean cumulative cost of breaches	Forrester research	$6,158,000	$6,158,000	$6,158,000
E3	Percentage of breaches originating from external attacks	Forrester research	49.1%	49.1%	49.1%
E4	Percentage of external attacks addressable with migrating to Azure	Forrester research	30%	30%	30%
E5	Annual risk exposure addressable with migrating to Azure	E1*E2*E3*E4	$807,295	$807,295	$807,295

E6	Reduced risk of breaches from external attacks with Microsoft Azure resilience guidance recommendations	Interviews	20%	20%	20%
Et	Improved security posture	E2*E3*E4	$161,459	$161,459	$161,459
	Risk adjustment	↓20%			
Etr	Improved security posture (risk-adjusted)		$129,167	$129,167	$129,167
	Three-year total: $387,502			**Three-year present value: $321,220**	

UNQUANTIFIED BENEFITS

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

- **Microsoft partnership.** Interviewees' partnership with Microsoft allowed them to be connected with access to technology expertise, scalable and secure infrastructure, a broad portfolio of solutions, a supportive ecosystem, integration capabilities, innovation opportunities, and trust and reliability. With extensive support resources, a strong commitment to security and compliance, and a focus on innovation, partnering with Microsoft empowered the interviewees' organizations to stay ahead of the curve, foster growth, and achieve their business objectives. The vice president and CISO at a financial services organization commented: "Well, I think Microsoft has had a pretty big impact. We've leaned on Microsoft quite a bit and their professional services organization to help us. I mean they're the ones that kind of stepped us through this Azure Data Services Well-Architected Review, and then we use them just generally for advisory services as we plan and execute our cloud migration."
- **Improved customer retention.** Interviewees noted that improving resilience and performance enabled them to improve customer satisfaction, which provided a competitive advantage. Customers rely on uninterrupted access to services and applications, and when uptime is consistently high, it builds trust and confidence in the brand. Improved uptime allows customers to work efficiently, meet their objectives, and minimizes the negative impact of downtime on their business operations. This reliability fosters customer satisfaction and loyalty, leading to higher retention rates. The vice president and CISO at a financial services organization commented, "For Azure apps where we used the Well-Architected

Framework, the customer retention went from the upper 80% range to the low 90% range."

- **Avoided penalty fees.** Interviewees discussed how Microsoft Azure resilience guidance recommendations improved SLAs, which helped organizations avoid penalty fees by setting clear performance metrics, raising performance standards, implementing monitoring and reporting processes, defining remediation procedures, and introducing financial incentives. Clear definitions and targets in SLAs aligned expectations between service providers and customers, while higher performance standards motivated service providers to maintain a higher level of service quality. The vice president and CISO at a financial services organization commented: "It depends on how badly you missed SLAs, but typically we're talking around 50% of the fees or the subscription cost for eight months. So in eight months, if you missed the SLA for one month, you're refunding the client half of what they paid you and that can be pretty substantial."

Avoided penalty fees

50%

"On a $5.2 billion top line revenue side, a 4.0 shift in customer retention is substantial."

VICE PRESIDENT AND CISO, FINANCIAL SERVICES

FLEXIBILITY

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

- **Creating a standard practice for re-architecting workloads.** Interviewees highlighted that after completing the Microsoft Azure resilience guidance recommendations, they are better equipped for architecting workloads in the future. They expect to benefit from consistency, quality assurance, time and cost savings, scalability, risk mitigation, knowledge management, and compliance to organizations by building a standard practice on architecting workloads. It ensures consistent design and implementation across the organization, saves time and effort, and allows for scalability and flexibility. Following established guidelines enables organizations to mitigate risks, deliver high-quality solutions, and meet regulatory requirements. Standard practices also facilitate knowledge sharing and training, enhance collaboration, and foster a culture of continuous learning.

  The vice president and CISO at a financial services organization commented, “We took a lot of the recommendations that came out of this, and after implementing them, if they achieved the expected benefit, then we basically made that a standard for all future so that we’re not basically having to do this assessment again and again.”

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

> “The documentation from Microsoft is by far the best. Microsoft spends a lot of time creating the documentation and it reflects the learning.”
>
> DIRECTOR, SOFTWARE ENGINEERING, COMMUNICATIONS AND IT

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**
Ftr	Initial re-architecting costs on Azure	$1,056,000	$0	$0	$0	$1,056,000	$1,056,000
Gtr	Ongoing management costs of critical workloads on Azure	$0	$1,299,375	$1,299,375	$1,299,375	$3,898,125	$3,231,353
	Total costs (risk-adjusted)	$1,056,000	$1,299,375	$1,299,375	$1,299,375	$4,954,125	$4,287,353

INITIAL RE-ARCHITECTING COSTS ON AZURE

Evidence and data. Interviewees described the initial labor costs related to re-architecting workloads on Azure across a variety of roles within the IT function. Data engineers, platform engineers, infrastructure experts, cloud engineers, and architects were typically involved in the re-architecting of workloads from the on-premises environments to the Azure cloud. On average, these individuals spent 50% of their time over the course of a six-month period.

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

- There are 20 architects involved in the initial re-architecting of critical workloads on Azure.
- Over the course of six months, 50% of their time is dedicated to re-architecting critical workloads after reviewing the principles of the Microsoft Azure resilience guidance.
- The average fully-burdened monthly salary of an architect is $16,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The number of architects involved in re-architecting workloads on Azure.
- Percentage of time dedicated to re-architecting workloads on Azure.
- The average fully-burdened monthly salary of an architect.

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 $1.1 million.

Initial Re-Architecting Costs On Azure						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Architects involved in initial re-architecting for critical workloads on Azure	Composite	20			
F2	Percentage of time dedicated to re-architecting critical workloads on Azure	Composite	50%			
F3	Months initially spent re-architecting workloads	Interviews	6			
F4	Average architect fully-burdened monthly salary	Composite	$16,000			
Ft	Initial re-architecting costs on Azure	F1*F2*F4	$960,000	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Initial re-architecting costs on Azure (risk-adjusted)		$1,056,000	$0	$0	$0
	Three-year total: $1,056,000		**Three-year present value: $1,056,000**			

ONGOING MANAGEMENT COSTS OF CRITICAL WORKLOADS ON AZURE

Evidence and data. Interviewees noted the involvement of system administrators in the ongoing management of Microsoft Azure resilience guidance recommendations as it related to maintaining critical workload performance on Azure. Given the extent of the documentation, interviewees noted the continuous use of Microsoft Azure resilience guidance recommendations to review any new updates. While some system administrators were more familiar with Azure than others, interviewees noted that some training was required as new recommendations and insights were shared from their Microsoft Azure resilience guidance assessments.

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

- There are 25 system administrators who spend 25% of their time on ongoing management of the Microsoft Azure resilience guidance for critical workload performance.
- These system administrators spend 10% of their time on ongoing training for any new principles and insights from the Microsoft Azure resilience guidance.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- The number of system administrators.
- The percentage of time dedicated to ongoing management and training of the Microsoft Azure resilience guidance recommendations.

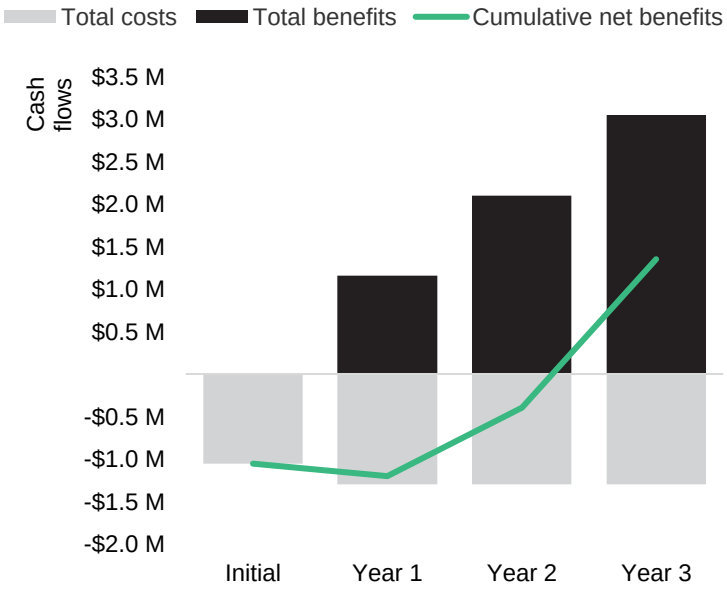
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.2 million.

Ongoing Management Costs Of Critical Workloads On Azure						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	System administrators managing critical workloads on Azure	C1		25	25	25
G2	Percentage of time dedicated to ongoing management of Microsoft Azure resilience guidance recommendations for critical workload performance	Composite		25%	25%	25%
G3	Average system administrator fully-burdened annual salary	Composite		$135,000	$135,000	$135,000
G4	**Subtotal: System administrator ongoing management costs**	**G1*G2*G3**		**$843,750**	**$843,750**	**$843,750**
G5	Percentage of time dedicated to training on new Microsoft Azure resilience guidance principles	Composite		10%	10%	10%
G6	**Subtotal: System administrator training costs**	**G1*G3*G5**		**$337,500**	**$337,500**	**$337,500**
Gt	Ongoing management costs of critical workloads on Azure	G4+G6		$1,181,250	$1,181,250	$1,181,250
	Risk adjustment	↑10%				
Gtr	Ongoing management costs of critical workloads on Azure (risk-adjusted)		$0	$1,299,375	$1,299,375	$1,299,375
	Three-year total: $3,898,125		**Three-year present value: $3,231,353**			

Financial Summary

Consolidated Three-Year Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



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	($1,056,000)	($1,299,375)	($1,299,375)	($1,299,375)	($4,954,125)	($4,287,353)
Total benefits	$0	$1,153,292	$2,101,480	$3,049,667	$6,304,439	$5,076,468
Net benefits	($1,056,000)	($146,083)	$802,105	$1,750,292	$1,350,314	$789,115
ROI						18%
Payback period (months)						27

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] Source: "How To Design Your Cloud-Native Patterns For Resilience," Forrester Research Inc., March 16, 2023.

[2] 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.

[3] Source: Forrester's Security Survey, 2022.

ABOUT FORRESTER CONSULTING

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

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

FORRESTER®