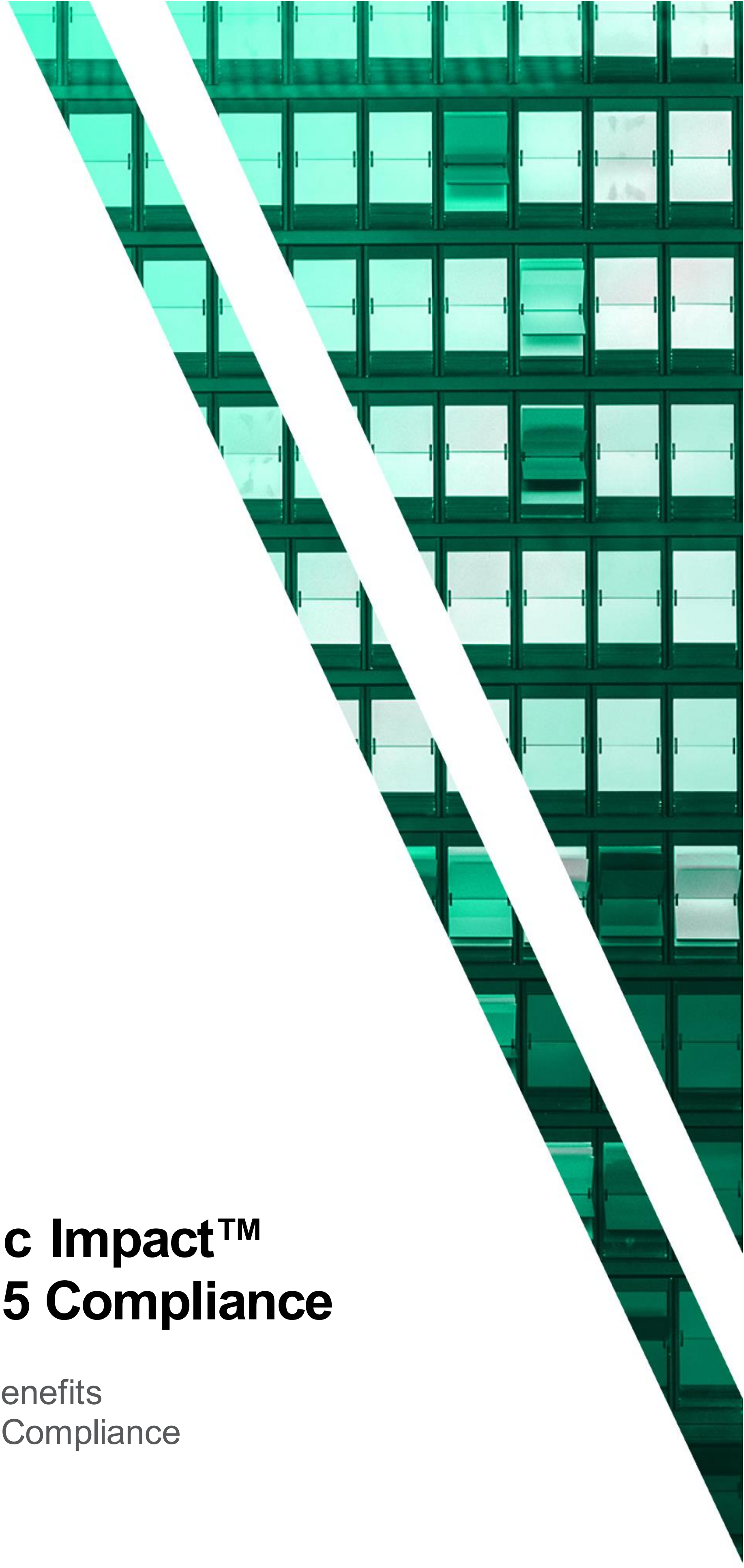
FORRESTER®



The Total Economic Impact™ Of Microsoft 365 E5 Compliance

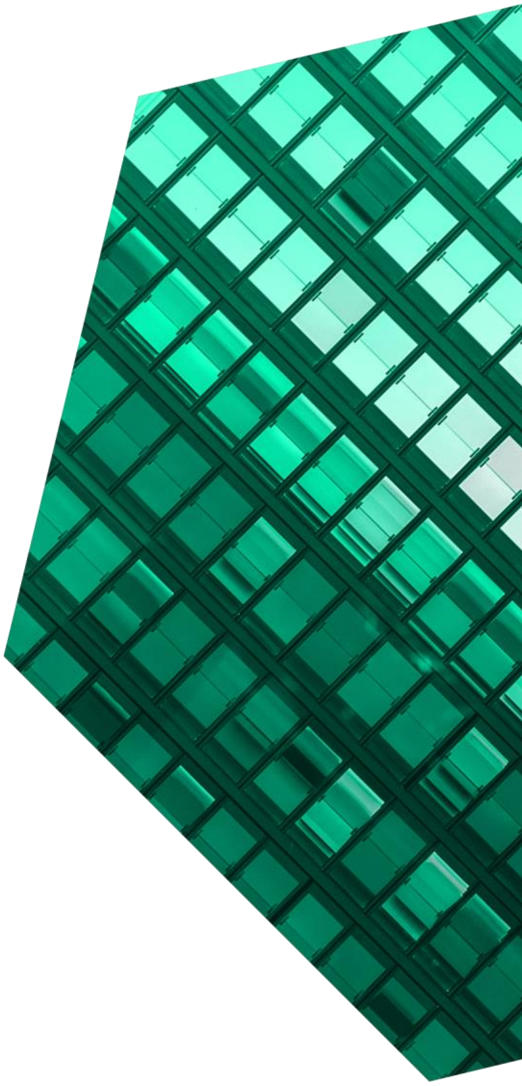
Cost Savings And Business Benefits Enabled By Microsoft 365 E5 Compliance

JUNE 2021

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY MICROSOFT

Table Of Contents

Consultant: *Mary Anne North*



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

Forrester's analysis of seven organizations using Microsoft 365 E5 Compliance reveals that they improved their ability to meet regulatory compliance requirements and reduced their risk of sensitive data loss or mishandling by providing better visibility and control through a single platform across compliance-related efforts and data. In addition, its workflows, dashboards, and AI enabled the organizations to increase employee productivity by streamlining their highly manual processes for managing compliance.

Microsoft 365 E5 Compliance is an integrated suite of compliance and risk management products that enables organizations to ensure and assess their compliance with regulatory requirements and to protect their sensitive data.

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Microsoft 365 E5 Compliance. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Microsoft 365 E5 Compliance on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed decision-makers from seven organizations with experience using Microsoft 365 E5 Compliance. The organizations operate in diverse industries including highly regulated ones like healthcare and energy, and their annual revenues range from $3 billion to $270 billion. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using Microsoft 365 E5 Compliance, the interviewed customers used multiple applications that each addressed some aspect of regulatory compliance (e.g., privacy, data retention). However, the customers felt those applications did not adequately reduce their regulatory compliance risk due to shortcomings in individual applications and an inability to gain full visibility of compliance efforts and statuses across those multiple applications. In addition, managing the various processes and data that was spread across those applications required considerable manual effort.

KEY STATISTICS

Return on investment (ROI)	Net present value (NPV)
46%	**$2.41M**

After investing in Microsoft 365 E5 Compliance, the customers were better able to comply with industry-specific and other regulatory requirements, improved the efficiency of their compliance-related processes, reduced the fees they pay to external service providers, and decreased the likelihood of a data breach and its potential cost.

KEY FINDINGS

The customer interviews and financial analysis found that a composite organization experiences benefits of $7.63 million over three years versus costs of $5.22 million, adding up to a net present value (NPV) of $2.41 million and an ROI of 46%.

Quantified benefits. Risk-adjusted present value (PV) quantified benefits applied to the composite organization and totaled over three years include:

- **Improved process efficiency valued at $3.1 million.** By streamlining and automating its processes around information protection and governance, risk management, and compliance management, the composite organization reduces manual effort by 85% to 90%. This saves it a total of 28,704 hours of manual effort in Year 1, which increases to 34,036 hours in Year 3.
- **Reduced external fees totaling $1.9 million.** The Advanced eDiscovery capabilities of Microsoft 365 E5 Compliance enabled the interviewees' organizations to reduce their volume of e-discovery content hosted for external legal review. By doing so, the organizations reduced the fees they paid to hosting providers and external legal counsel, and the savings increased over time as the volume of applicable corporate data grew. The composite organization experiences a 60% reduction in the volume of hosted content, with a corresponding 60% decrease in fees for both external hosting and external legal review. Because Microsoft 365 E5 Compliance enables external auditors to compile needed data and to gain visibility into compliance status more rapidly, the interviewees' organizations also paid less in external auditor fees. The composite organization saves $110,000 in external audit fees in Year 1, which increases to $120,000 by Year 3.
- **Decreased risk and cost of a data breach valued at $409,953.** Interviewees said their organizations used a number of Microsoft 365 E5 Compliance capabilities that combined to reduce both the risk of certain kinds of data breaches and the cost if a breach did occur. The composite organization experiences a 30% to 40% reduction in risk and a 40% to 50% reduction in the cost, cutting its expected average annual cost of a breach from a baseline of $287,570 to $86,271 in Year 3.

> **"We sleep better now because we realize we're safer."**
>
> *Manager of legal applications, energy*

- **Cost savings of $2.3 million from retiring legacy third-party software.** Deploying Microsoft 365 E5 Compliance enabled the interviewees' organizations to retire their previous on-premises compliance software and eliminate the costs of infrastructure, upgrades, and IT staff associated with that software.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Ease of adoption, use, and administration from having a single integrated solution.** Consistency across the Compliance suite and integration with the organizations' existing Microsoft platforms simplified the learning curve and ongoing use.
- **Visibility and audit history of data and workflows across the full suite.** By replacing multiple tools with a single suite, each of the interviewees' organizations gained a unified picture of its compliance status and activities.
- **The bandwidth to be more proactive and strategic, instead of reactive.** The process efficiencies enabled by Microsoft 365 E5

Compliance allowed staff to reallocate time spent on repetitive and often reactive manual processes to higher-level and more strategic initiatives.

- **Greater ease and consistency in compliance reporting.** The integrated tools and data delivered by Microsoft 365 E5 Compliance reduced the time the interviewees' organizations needed for reporting, and they improved the consistency of those reports.

> **"People are amazed at the things we can now report on and the information we can give them."**
>
> *Head of cybersecurity, natural resources*

- **Improved ability to anticipate and respond to compliance requirements of international expansion.** When the interviewees' organizations expanded into additional countries, the frameworks and tools of Microsoft 365 E5 Compliance helped them understand and implement country-specific regulations and compliance requirements.
- **Shorter turnaround times on information requests and legal processes.** The interviewees' organizations gained the ability to respond to internal or external requests for information much more quickly because they now have access to all the pertinent information in one place along with an integrated set of tools.

Costs. Risk-adjusted PV costs applied to the composite organization and totaled over three years include:

- **Microsoft fees of $4.3 million.** Microsoft 365 E5 Compliance subscription fees vary depending on the number of licensed users and the organization's purchase structure (e.g., whether it purchases individual E5 Compliance modules or the full E5 Compliance suite, or if it gains access to E5 Compliance as part of an overall Microsoft 365 E5 purchase or an upgrade from Microsoft 365 E3).
- **Internal labor for implementation, management, optimization, and support totaling $883,566.** Initial internal labor costs for the composite organization include 2,500 hours of staff time, 20 hours of training for each of the 40 power users, and 45 minutes of training for each employee. Ongoing annual costs include 2,000 hours of staff time for management, optimization, and support, and 6 hours of training for each of the 40 power users.

Now that we use a single suite of compliance products, defining compliance requirements and managing compliance has all gotten a lot simpler.

— VP of IT and cybersecurity, information services

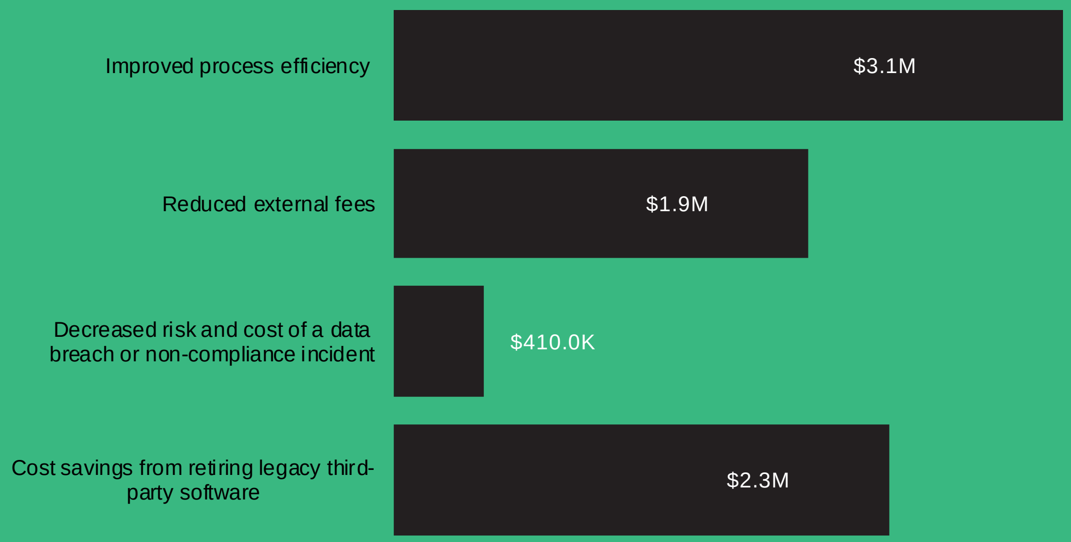
ROI
46%

BENEFITS PV
$7.63M

NPV
$2.41M

PAYBACK
11 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 Microsoft 365 E5 Compliance.

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 365 E5 Compliance 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 365 E5 Compliance.

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.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft 365 E5 Compliance.

CUSTOMER INTERVIEWS

Interviewed nine decision-makers at seven organizations using Microsoft 365 E5 Compliance to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

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 365 E5 Compliance Customer Journey

🟩 Drivers leading to the Microsoft 365 E5 Compliance investment

Interviewed Organizations

Industry	Revenue	Region	Interviewee	Modules deployed
Energy	$140 billion	North America with global operations	Manager of legal operations	Compliance management, Information protection & governance
Professional services	$3 billion	North America with global operations	CISO, director of information services, senior director of IT security	Compliance management, Information protection & governance, Risk management
Natural resources	$6 billion	Asia with global operations	Head of cybersecurity	Compliance management, Information protection & governance, Risk management
Energy	$270 billion	EMEA with global operations	Compliance lead	Compliance management, Information protection & governance
Retail	$6 billion	North America with global operations	VP of IT	Compliance management, Risk management
Information services	$30 billion	North America with global operations	VP of IT and cybersecurity	Compliance management, Information protection & governance, Risk management
Healthcare	$5 billion	North America with regional operations	Director of IT	Compliance management, Information protection & governance, Risk management

KEY CHALLENGES

Prior to deploying Microsoft 365 E5 Compliance, the interviewees' organizations used a combination of several third-party software packages to address various aspects of compliance. The organizations struggled with common challenges, including:

- **Lack of visibility into compliance posture and limited capability to assess and manage regulatory compliance.** Because of the fragmentation created by using multiple tools to address various aspects of regulatory compliance, the organizations lacked visibility to their overall compliance postures and the current status of their compliance with specific regulations. They could not readily enforce controls, proactively gauge the status of their compliance, or track the progress of assessments, audits, and remediation efforts. A manager of legal applications for an energy company said: "We had no ability to confirm that what we told another group to do was actually being done. We would throw it out there into the ether and hope somebody did it." A VP of IT and cybersecurity at an information services company said: "We were paying millions of dollars in fines because we were unable to remediate critical audit findings. We had no central visibility as an enterprise to our global regulatory requirements." A director of IT at a healthcare organization said: "We never really knew how compliant we were.

> **"One tool did one thing, and another tool did another thing. Those tools didn't really talk, and you had to try to put them all together manually."**
>
> *Manager of legal applications, energy*

Spot checks across facilities often identified discrepancies. A lot depended on how well a particular site was staffed."

> **"Our prior solutions were not giving us an accurate picture. That left us vulnerable to material risks, which isn't a good thing for a public company."**
>
> *Head of cybersecurity, natural resources*

- **Inadequate protection against regulatory risk.** The interviewees said their organizations' previous solutions did not provide sufficient protection against a range of internal and external risk factors that impact regulatory compliance, or the ability to pinpoint and address suboptimal practices.
- **Resource optimization and efficiency.** With data and regulations both proliferating, the interviewees' organizations couldn't keep up.

> **"We wanted to have our internal resources working on innovation and strategic projects — not just 'keep the lights on' efforts."**
>
> *VP of IT, retail*

Navigating the regulatory landscape and ensuring and demonstrating compliance required extensive manual effort across multiple tools with different access mechanisms (sometimes just spreadsheets) that diverted staff from more strategic, higher-level endeavors. The director of IT at the healthcare organization provided several examples of tedious manual work, such as putting together documentation, presentations, and reports, and having to enter new or revised regulations into each facility's system instead of using an automated, organizationwide approach.

- **Compliance speedbumps on the road to business/digital transformation**. Interviewees said their previous compliance solutions did not adequately support their organizations' business/digital transformation efforts, including the increased reliance on remote workforces.

> **"We needed tools that would help secure our remote workforce and our overall digital transformation."**
>
> *CISO, professional services*

COMPOSITE ORGANIZATION

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

Description of composite. The composite organization generates $8 billion in annual revenue in a highly regulated industry, and it operates globally. Its applications and data are hosted both in the cloud and on-premises, but most are in the cloud. The organization must comply with numerous regulations and standards around privacy, data protection, and preservation of documents (e.g., General Data Protection Regulation [GDPR], Personally Identifiable Information [PII], Payment Card Industry Data Security Standard [PCI-DSS], and Health Insurance Portability and Accountability Act [HIPAA] regulations) at the regional, state, and national levels.

Key assumptions

- $8 billion in annual revenue
- Highly regulated industry
- Global operations

Deployment characteristics. The organization gains access to Microsoft 365 E5 Compliance as part of its overall move from Microsoft 365 E3 to Microsoft 365 E5. It implements the full Microsoft 365 E5 Compliance suite using internal resources and informal assistance from Microsoft. It deploys elements of the suite's information protection and governance and risk management capabilities across the entire workforce. It also provides employees in IT, the legal department, HR, and other functions with enhanced access to one or more of those capabilities and/or access to other capabilities and/or access to other capabilities within the suite as needed. Implementation includes 1 hour of training for all employees about the information protection and governance capabilities and several days of training for individuals in roles that work extensively with any of the suite's capabilities. A team of representatives from those functions continues to optimize its use and leverages new capabilities as they are released. Microsoft 365 E5 Compliance requires minimal technical support on an ongoing basis.

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 process efficiency	$1,123,762	$1,255,854	$1,332,509	$3,712,125	$3,060,631
Btr	Reduced external fees	$720,000	$765,000	$810,000	$2,295,000	$1,895,342
Ctr	Decreased risk and cost of a data breach or non-compliance incident	$150,008	$166,335	$181,169	$497,512	$409,953
Dtr	Cost savings from retiring legacy third-party software	$790,920	$1,150,920	$790,920	$2,732,760	$2,264,422
	Total benefits (risk-adjusted)	$2,784,689	$3,338,109	$3,114,599	$9,237,397	$7,630,348

IMPROVED PROCESS EFFICIENCY

Evidence and data. By deploying Microsoft 365 E5 Compliance, the interviewees' organizations improved the efficiency of their processes around information protection and governance, risk management, and compliance management. For the composite organization, these efficiency improvements save a total of 28,704 hours of manual effort in Year 1, which increases to 34,036 hours in Year 3.

The increase over time is attributable to both the organization's expanded and more informed use of Microsoft 365 E5 Compliance's capabilities and the AI learning (especially during Year 1) that underlies and amplifies the impact of certain capabilities.

The efficiencies are driven by replacing multiple tools with a single compliance platform that covers a full range of a company's compliance operations and much of its pertinent data, as well as specific Microsoft 365 E5 Compliance capabilities for information protection and governance, risk management, and compliance management.

By using a single integrated suite of compliance capabilities, the interviewees' organizations streamlined their compliance processes. The VP of IT and cybersecurity at the information services company said: "We now have access to all of our compliance efforts and data in a single suite, instead of going crazy accessing different products from different vendors with different access mechanisms. The interoperability among various capabilities also saves effort, like transferring data between e-discovery and insider risk functions to manage an insider risk case. We can make sense of the data because everything speaks the same language instead of different languages that we have to parse among multiple products. It's saving time across our audit, security, legal, and other teams."

Information protection and governance refers to safeguarding sensitive data. Microsoft 365 E5 Compliance's information protection and governance capabilities include data loss prevention (identifying and protecting sensitive information); message encryption; data classification; records management (retention, deletion); remediation; auditing and testing; and defining and implementing controls.

The interviewees described a number of ways in which Microsoft 365 E5 Compliance reduced their organizations' manual effort around information protection and governance. Automatic discovery and classification of sensitive data, along with application of sensitivity labels, through AI replaced what typically had been manual effort to identify, classify, and segregate sensitive data. A compliance lead at an energy company estimated that previously about 20,000 employees spent an average of 20 minutes each day moving documents from office productivity tools into a secure document storage system. With Microsoft 365 E5 Compliance, secure storage happens in place.

Similarly, the organizations replaced manual effort to classify data for access and retention with automatic classification of data based on the product's Exact Data Match or Machine Learning. With Machine Learning, organizations used "trainable classifiers" to automatically apply default retention labels to certain sets of data and automatically apply retention policies based on specific conditions such as keywords, content types, or sensitive information. They could more rapidly review and validate dispositions, then export information about all disposed items.

A manager of legal applications at an energy company indicated that company previously needed one-half of a dedicated information governance FTE in each business unit to ensure retention policies were applied and data got deleted when necessary. With AI now enabling those tasks, that time is now available for other initiatives.

That same energy company previously conducted a yearly manual review of documents targeted for disposition, with five people working full-time for one month. Because Microsoft 365 E5 Compliance enabled moving most retention categories to automatic disposition, 95% of that effort was eliminated.

Microsoft 365 E5 Compliance also reduced the time needed to remediate a risk incident, i.e., alerting management, HR, and legal, and then gathering, packaging, and sharing pertinent information. A VP of IT at a retail company explained that the product saved considerable time by specifying what kind of information needed to be gathered and from where, depending on the nature of the incident.

Interviewed organizations noted the ease of updating, redefining, and implementing controls across their operations, with Microsoft 365 E5 Compliance's single integrated suite.

> **"By implementing controls at a platform level, we don't have to go figure out how to implement the same control into multiple systems."**
>
> *CISO, professional services*

Risk management refers to identifying and remediating critical risks around code-of-conduct policy violations and internal threats and data leakage. Microsoft 365 E5 Compliance capabilities include insider risk management, communication compliance, Advanced Audit, information barriers, Privileged Access Management, and Customer Lockbox.

Interviewees provided the following examples of how Microsoft 365 E5 Compliance reduced risk management effort at their organizations:

- With compliance and other risk information centralized in a single location, a natural resources company decreased the time spent on ongoing monitoring and checking indicators of potential suspicious activity from 12 hours per week to 30 minutes per week. That's a 96% reduction. Previously, several incidents each quarter would require deeper investigation by a team of five people working full time for two weeks. Now, that team spends just three days per incident, which is a 70% reduction.

- The VP of IT at the retail company said their organization replaced spreadsheet-based access management (which was used by managers up to the SVP level) with a more automated approach. They said, "It's one click to indicate 'I approve' or 'I don't approve this one person' instead of all the time-consuming, manual back-and-forth we used to have."
- The VP of IT and cybersecurity at the information services company said Microsoft 365 E5 Compliance saved their organization time in identifying risks and investigating alerts. Because information is automatically pulled into a central location (Microsoft 365 E5 Compliance), the company's security team no longer had to gather information from multiple tools to identify risks and investigate alerts. The interviewee said specific tasks that take less time include identifying critical insider risks, identifying and investigating alerts, remediating risk incidents (i.e., alerting management, HR, and the legal department and gathering, packaging, and sharing pertinent info), ensuring communications compliance by using natural-language processing to automatically monitor inappropriate communications, and restricting access and information flows by establishing information barriers and privileged access management.

Compliance management refers to assessing regulatory compliance and responding to legal and regulatory requirements. Microsoft 365 E5 Compliance's compliance management capabilities include Microsoft's Advanced eDiscovery solution and Compliance Manager. Compliance Manager includes features such as tracking for regulatory and standards changes, implementing and updating data protection controls (specified by compliance, security, privacy, and data protection standards and regulations), assessing compliance with standards and identifying and assessing risks of non-compliance by using automatic assessment via Compliance Manager, complying with audit requirements, and preparing regulatory reports.

Microsoft 365 E5's Advanced eDiscovery solution saves time for internal legal teams and IT forensics groups around document preservation, collection, and review.

- A manager of legal applications at an energy company said their organization initiates an average of 900 discovery processes each year, leading to 10,000 people becoming the subject of forensics inquiries. For each of those people, the legal team previously had to submit a request to the IT department to collect mailboxes, personal drives, and other data. An e-discovery project manager would create a request that described the needed info, send the request to the forensics IT team, and then check the information that came back.

  With Microsoft 365 E5 Compliance, those e-discovery project managers gained the ability to access the information themselves in real time, so handoffs and quality control checks are no longer needed. What previously required a total of 30 minutes of effort from a project manager for each request can now be done in a minute or two – a 93% to 97% time reduction – and without a delay while waiting for information to be returned.

> **"Discovery requests previously required exporting people's mailboxes into a separate tool. Now it all happens in place."**
>
> *CISO, professional services*

- A compliance lead at an energy company said their organization's efforts to preserve, collect, and review custodian documents previously required a team of eight preservation coordinators. With Microsoft 365 E5 Compliance, a three-person team can handle it.
- The VP of IT and cybersecurity at the information services company said e-discovery work that previously took a total of 40 hours per week across legal, audit, and security teams now takes 15 hours per week, for a 63% reduction. The interviewee said having one central repository for all legal hold documents saved time on forensic and compliance investigations by making it easier to preserve, collect, and review custodian documents.
- The director of IT at the healthcare organization said their organization's time to investigate a suspicious incident dropped by 67% from 3 hours to 1 hour.

The interviewees also described many ways in which the compliance management capabilities of Microsoft 365 E5 Compliance saved manual effort for their organizations. This included tracking regulatory and standards changes and making those changes visible to multiple groups across the organizations, automatically determining compliance scores, and automatically generating reports for use internally or by external auditors. Examples include:

- The VP of IT and cybersecurity at the information services company said having a "single pane of glass" view of compliance helped their organization decrease the time spent creating reports by 96%. Instead of requiring 40 business units to spend 10 hours each on the task for a total of 400 hours, one centralized team now creates the reports in 15 hours each week.
- The director of IT at the healthcare organization said their organization saw an 83% reduction in manual effort by risk analysts and directors of risk management to put documentation, reports, and presentations together and to adjust systems to reflect new or changed regulations.
- A director of information services at a professional services firm said a new regulation or a major change to an existing regulation typically surfaces three to four times each year. Each time, the organization's resulting analysis of controls and how they apply to data would previously require a total of 240 hours of manual effort. With Microsoft 365 E5 Compliance and a process created with about 35 hours of development effort using the included Microsoft Power BI Pro, the company cut that effort by 97% to a total of 8 hours.
- The head of cybersecurity for a natural resources organization said their company previously spent 40 hours at least twice per year to compile and format the necessary information to comply with both internal and external auditing requirements. It now spends 90 minutes each time, which is a 96% reduction.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Prior to deployment, individuals across the organization annually spend a total of 20,000 hours on information protection and governance, 4,160 hours on risk management, and 15,000 hours on compliance management.
- By using Microsoft 365 E5 Compliance over three years, the organization reduces manual effort by:
  - 70% to 85% for information protection and governance.
  - 65% to 85% for risk management.
  - 80% to 90% for compliance management.

Risks. Improved process efficiency will vary based on:

- The degree of automation of prior processes.
- The capabilities of prior compliance software.
- The extent to which the organization leverages the capabilities of Microsoft 365 E5 Compliance and further matures its compliance operations.
- The number of employees in compliance-related roles.
- Prevailing local compensation rates.

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 $3,060,631.

Improved Process Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Baseline annual time spent on information protection and governance before Compliance (hours)	Interviews	20,000	20,000	20,000
A2	Reduction in effort	Interviews	70%	80%	85%
A3	Improved process efficiency for information protection and governance (hours of effort saved)	A1*A2	14,000	16,000	17,000
A4	Baseline annual time spent on risk management before Compliance (hours)	Interviews	4,160	4,160	4,160
A5	Reduction in effort	Interviews	65%	80%	85%
A6	Improved process efficiency for risk management (hours of effort saved)	A4*A5	2,704	3,328	3,536
A7	Baseline annual time spent on compliance management before Compliance (hours)	Interviews	15,000	15,000	15,000
A8	Reduction in effort	Interviews	80%	85%	90%
A9	Improved process efficiency for compliance management (hours of effort saved)	A7*A8	12,000	12,750	13,500
A10	Total time of effort saved (hours)	A3+A6+A9	28,704	32,078	34,036
A11	Productivity captured from time saved	Forrester	75%	75%	75%
A12	Blended, fully burdened hourly compensation of employee	Assumption	$58	$58	$58
At	Improved process efficiency	A10*A11*A12	$1,248,624	$1,395,393	$1,480,566
	Risk adjustment	↓10%			
Atr	Improved process efficiency (risk-adjusted)		$1,123,762	$1,255,854	$1,332,509
	Three-year total: $3,712,125		**Three-year present value: $3,060,631**		

REDUCED EXTERNAL FEES

Evidence and data. The interviewees said using Microsoft 365 E5 Compliance reduced their organizations' fees for e-discovery external hosting, external legal review of hosted e-discovery content, and external auditors' efforts. For the composite organization, this combined savings grows from $720,000 in Year 1 to $810,000 in Year 3 as the overall volume of pertinent data subject to e-discovery grows.

Each lawsuit filed against an organization triggers a discovery process that includes gathering relevant documents, including emails of the involved employees. That content gets exported and hosted externally for review by external legal counsel.

The Advanced eDiscovery capabilities within Microsoft 365 E5 Compliance use machine learning and advanced analytics to stop repeating the same email message in multiple email threads, to cluster documents of similar types together for deduplication, and to organize content to make the review process more efficient. The VP of IT at the retail company said: "We now can do a better job of determining what external counsel really needs to see. We no longer give them five copies of the same email."

Since e-discovery hosting providers charge by the gigabyte, decreasing the volume of hosted content cuts hosting costs. Similarly, reducing the volume of documents subject to external legal review and better organizing them cuts the number of hours that law firms must charge for a review.

Interviewees said their organizations now pay less in external auditor fees (typically billed as time and expenses) because Microsoft 365 E5 Compliance enables their auditors to compile the necessary data and to gain visibility into compliance status more rapidly. The VP of IT and cybersecurity at the information services company said: "We save a lot of money because auditors get what they need quickly instead of running around the company trying to figure out who can give them the information." In addition, some of the interviewees said their organizations previously tapped their external auditors to handle tasks that could have been addressed internally if their compliance employees had the bandwidth to do so.

> **"Because we can refine how much data we have to export, there's less cost for the external hosting and outside counsel review of that data."**
>
> *Manager of legal applications, energy*

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The overall volume of corporate data that may be subject to e-discovery external hosting, external legal review, or auditor efforts grows each year.
- The baseline annual fees for e-discovery external hosting increase from $400,000 in Year 1 to $450,000 in Year 3.
- The baseline annual fees for external legal review of hosted e-discovery content increase from $750,000 in Year 1 to $850,000 in Year 3.
- Microsoft 365 E5 Compliance reduces the volume of hosted and reviewed content by 60%.
- The organization saves $110,000 on external audit fees in Year 1, which increases to $120,000 in Year 3.

Risks. The reduction in external fees will vary based on:

- The organization's size and industry.
- The organization's level of process maturity.
- The volume of data reviewed.
- The extent to which the organization leverages the capabilities of Microsoft 365 E5 Compliance and further matures its compliance operations.
- Prevailing local rates for hosting providers, external legal counsel, and external auditors.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1,895,342.

Reduced External Fees

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Baseline annual fees for e-discovery external hosting	Interviews	$400,000	$425,000	$450,000
B2	Reduction in volume of hosted content	Interviews	60%	60%	60%
B3	Reduction in fees for e-discovery external hosting	B1*B2	$240,000	$255,000	$270,000
B4	Baseline annual fees for external legal review of hosted e-discovery content	Interviews	$750,000	$800,000	$850,000
B5	Reduction in volume of reviewed content	Interviews	60%	60%	60%
B6	Reduction in fees for external legal review	B4*B5	$450,000	$480,000	$510,000
B7	Reduction in external audit fees	Interviews	$110,000	$115,000	$120,000
Bt	Reduced external fees	B3+B6+B7	$800,000	$850,000	$900,000
	Risk adjustment	↓10%			
Btr	Reduced external fees (risk-adjusted)		$720,000	$765,000	$810,000
	Three-year total: $2,295,000		Three-year present value: $1,895,342		

DECREASED RISK AND COST OF A DATA BREACH OR NON-COMPLIANCE INCIDENT

Evidence and data. By deploying Microsoft 365 E5 Compliance, the interviewees' organizations not only reduced their risk of certain kinds of data breaches, but they also reduced the likely cost if a breach did occur. The composite organization experiences a 30% to 40% reduction in risk, and a 40% to 50% reduction in the cost, cutting its expected average annual cost of a breach from a baseline of $287,570 to $86,271 in Year 3.

Specific types of data-breach incidents include exposing sensitive data (for example: when unauthorized internal or external users gain access to proprietary data, PII, or other sensitive data), and violating data protection, privacy, or disclosure laws like GDPR HIPAA, which can lead to paying regulatory fines.

The head of cybersecurity at the natural resources company said: “Microsoft 365 E5 Compliance reduces our risk because the more of its features we use — especially around data protection and information governance — then the better visibility and controls we have. That reduces the likelihood of breaches happening. And if there is a breach, we’re better able to catch things early and respond quickly.”

Interviewees said a number of Microsoft 365 E5 Compliance capabilities combine to reduce the risk of a data breach, including:

- **Improved visibility to risks.** A manager of legal applications at an energy company said: “Previously, we didn’t have a whole lot of visibility or even insight into the metrics we should capture to ensure we are doing things correctly. Having everything in one place has helped us identify potential risks of compliance gaps.” A head of cybersecurity at a natural resources company said: ”We see the entire picture now. [Microsoft 365 E5 Compliance] has opened up a whole new way of looking at areas we need to protect better.”

- **Autoclassification of sensitive corporate data.** Microsoft 365 E5 Compliance auto classifies sensitive corporate data like payment/credit card data, PII (e.g., name, address, phone number, Social Security number), and account numbers, and it prevents end users from deliberately or inadvertently emailing that sensitive data. A manager of legal applications at an energy company said: “Using AI to automatically identify sensitive information helps keep it more secure. You’re not relying on the end user to make that determination.”

- **Autoremediation capabilities.** The VP of IT and cybersecurity at the information services company said the autoremediation capabilities of Microsoft 365 E5 Compliance made it possible to block and flag an employee’s attempt to push highly sensitive data to an external person, thereby preventing a possible breach and alerting the need for supervisors to follow up with that employee. The VP also said their organization now has the ability to track how many critical events Microsoft 365 E5 Compliance has auto remediated.

> **“Through the dashboard, we can actually see the number of things that potentially could have been lost but that were instead protected.”**
>
> *Head of cybersecurity, natural resources*

- **Better ability to restrict access to sensitive data.** Interviewees said Microsoft 365 E5 Compliance improved their organizations’ abilities to ensure that only authorized users access sensitive or confidential data.

- **Improved records management.** Interviewees said Microsoft 365 E5 Compliance simplified records management in term of both retention (e.g., what needs to be retained to avoid fines) and deletion. They also noted that retaining records longer than required increases their organizations’ risks of exposing sensitive data. The director of IT at the healthcare organization said: “We have document retention policies. But just because it’s a policy, it doesn’t necessarily mean it’s followed by everyone. Accidents do happen. People do leave the organization. Having one dashboard — one system — where all that compliance-related information coincides makes it easier to track and manage.”

- **Lower volume of sensitive data exposed externally during litigation e-discovery.** By using the capabilities of Microsoft Advanced eDiscovery to decrease the volume of data that gets hosted and reviewed externally during litigation, the interviewees' organizations decreased the amount of sensitive data that is outside of their custody and control. A manager of legal applications at an energy company said: "Some of our service providers have had data breaches. Luckily, none of our data got out. But some of that data is very sensitive. We're able to limit that data to be very narrow in scope. So, we're not putting irrelevant things out in the wild to be potentially exploited."

- **Improved insider risk management.** Interviewees said their organizations gained more ability to monitor suspicious data access by employees. The head of cybersecurity at the natural resources company said: "When we know an employee will be leaving the company, we can now monitor them more closely for anything that looks a bit suspicious — whether that's copying data to private drives, sending emails to private email addresses, or uploading or downloading massive [amounts of] data."

Similarly, interviewees said a number of factors would reduce the cost of a breach if one does occur by enabling their organizations to spend less time and money managing a breach and to recover faster and more completely. Those factors include:

- **Decreased manual effort around e-discovery.** Microsoft 365 E5 Compliance enabled a more automated approach to e-discovery and reduced staff time spent gathering pertinent data and documents.

- **Reduced reputational damage, customer lawsuits, and revenue loss.** With Microsoft 365 E5 Compliance, the interviewees' organizations could respond to incidents more quickly, and that included identifying affected parties for notification. Having a faster response time can decrease the brand damage caused by a breach, including lost revenue from customer loss, costs to rebuild brand equity, and costs to acquire new customers. It also can reduce the amount of customer lawsuits and the resulting compensation and punitive damages.

> **"What's ultimately at stake is our continued existence as a firm and all of our revenue. Would we still be in business with the reputational damage?"**
>
> *CISO, professional services*

- **Reduced regulatory fines due to more timely response and the ability to demonstrate a strong compliance posture.** Regulatory and compliance measures that an organization may need to follow can affect that organization financially if a security breach happens. To avoid paying fines or to lessen them, organizations may be required to take certain actions (e.g., notify affected customers) within a prescribed time period after a breach.

  The head of cybersecurity at the natural resources company said: "Some of the regulatory bodies we have to report to need to be notified within 72 hours after certain events. With our disparate previous systems, sometimes we were finding things out after 72 hours and having to pay fines." The imposition or extent of those fines may vary depending on whether or not an organization can demonstrate that it adhered to sound compliance and security practices. A CISO at a professional services firm said the controls provided by Microsoft 365 E5 Compliance may reduce the risk of fines because it can help decision-makers understand and address the reason the fine was imposed.

- **Additional audit and security compliance costs.** A breach may subject an organization to incremental audit and security compliance costs going forward.

Forrester's approach to valuing the decreased risk and cost of a data breach is conservative, reflecting an array of incident types and costs. Depending on the organization's industry, geographic focus, and operational processes, both risk and costs will vary.

> **"If something bad does happen we now can do what we need to do faster and better."**
>
> *Director of IT, healthcare*

For instance, a GDPR violation for organizations operating in the European Union could lead to a fine of up to €20 million or 4% of that organization's worldwide annual revenue from the preceding financial year, whichever amount is more.[1]

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The average cost of a data breach is more than $3.8 million.[2]
- The likelihood of a 30,000-record data breach in a given year is 7.45%.[3]
- By deploying Microsoft 365 E5 Compliance, the organization:
  - Reduces the cost of a data breach by 40% in Year 1, by 45% in Year 2, and by 50% in Year 3.
  - Reduces the likelihood of a data breach in a given year by 30% in Year 1, by 35% in Year 2, and by 40% in Year 3.

Risks. The decreased risk and cost of a data breach will vary based on:

- The prevalence, nature, and average cost of data breaches in the organization's industry.
- The geographic scope of the organization's operations.
- The regulatory and compliance measures the organization is required to follow.
- The organization's prior state and maturity level for compliance.
- Previously used compliance software.
- The extent to which the organization leverages the capabilities of Microsoft 365 E5 Compliance and further matures its compliance operations.
- The maturity level of the organization's information security.
- The volume and type of data breached.
- How quickly the organization can respond to a breach

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $409,953.

Decreased Risk And Cost Of A Data Breach Or Non-Compliance Incident					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Average cost of a data breach (global)	Ponemon 2020	$3,860,000	$3,860,000	$3,860,000
C2	Likelihood of a 30,000-record breach (within 2 years/2)	Ponemon 2019	7.45%	7.45%	7.45%
C3	Expected average annual cost of a breach before Compliance	C1*C2	$287,570	$287,570	$287,570
C4	Reduction in cost from using Compliance	Interviews	40%	45%	50%
C5	Reduction in likelihood after Compliance	Interviews	30%	35%	40%
C6	Average cost of a data breach after Compliance	(1-C4)*C1	$2,316,000	$2,123,000	$1,930,000
C7	Average likelihood of a data breach after Compliance	(1-C5)*C2	5.22%	4.84%	4.47%
C8	Expected average annual cost of a breach after Compliance	C3-C8	$120,895	$102,753	$86,271
Ct	Decreased risk and cost of a data breach or non-compliance incident	C3*C4	$166,675	$184,817	$201,299
	Risk adjustment	↓10%			
Ctr	Decreased risk and cost of a data breach or non-compliance incident (risk-adjusted)		$150,008	$166,335	$181,169
	Three-year total: $497,512		**Three-year present value: $409,953**		

COST SAVINGS FROM RETIRING LEGACY THIRD-PARTY SOFTWARE

Evidence and data. After deploying Microsoft 365 E5 Compliance, the interviewees' organizations were able to retire their previous on-premises compliance software. This eliminated not only the ongoing costs of the on-premises infrastructure (e.g., hardware, software, associated maintenance charges), but also the costs of IT staff time needed to support that infrastructure. It also eliminated the effort and expense needs of upgrading that infrastructure every few years. As a result, the composite organization saves $790,920 in Year 1, $1,278,800 in Year 2, and $790,920 in Year 3.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- The previous annual software maintenance fees totaled $500,000.
- The previous annual infrastructure costs for the legacy software totaled $150,000.
- Infrastructure upgrades previously cost $400,000 every third year.
- Two IT support FTEs previously managed, maintained, and supported the legacy software.

Risks. Cost savings from retiring legacy third-party software will vary based on:

- The number and nature of the organization's legacy software programs.
- The number of resources managing the legacy systems that can be reallocated.
- The scope of the organization's operations.
- The infrastructure needed for the legacy software.

- The frequency and extent of upgrades for the legacy software.
- The internal labor needed to manage the legacy software.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2,264,422.

Cost Savings From Retiring Legacy Third-Party Software

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Software maintenance fees	Interviews	$500,000	$500,000	$500,000
D2	Annual infrastructure costs for legacy solutions	Interviews	$150,000	$150,000	$150,000
D3	Periodic infrastructure upgrade costs for legacy solutions	Interviews	$0	$400,000	$0
D4	IT support FTEs required	Interviews	2	2	2
D5	Fully burdened annual compensation for IT FTE	Assumption	$114,400	$114,400	$114,400
Dt	Cost savings from retiring legacy third-party software	D1+D2+D3+ (D4*D5)	$878,800	$1,278,800	$878,800
	Risk adjustment	↓10%			
Dtr	Cost savings from retiring legacy third-party software (risk-adjusted)		$790,920	$1,150,920	$790,920
Three-year total: $2,732,760			Three-year present value: $2,264,422		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Ease of adoption, use, and administration from having a single integrated solution.** The director of information services at the professional services firm said: “Now we don’t have to ask: ‘Can this product be integrated? Can we get the stuff out of it that we need? Is it going to require some separate authentication?’ With Microsoft, things are consistent across the entire suite.” The CISO at the same firm said: “The access control is all centralized. It’s all the same data set and a connected set of features. Since everything integrates into a platform we already have, we don’t have to make a lot of changes or learn a new interface; we just need to learn the incremental functionality. There’s a familiarity that cuts the learning curve.”
- **Visibility and audit history of data and workflows across the full suite.** By replacing multiple tools with a single suite, each of the organizations gained a unified picture of its compliance status and activities. A manager of legal applications at an energy company said: “We now have valuable audit trails, so we can prove things happened as they should have.”

  Interviewees said their organizations could also gather compliance-related data from multiple sources more easily. The head of cybersecurity at the natural resources company said: “We can do e-discovery across our various sources and pull in all the data to get an overall picture of a user or an event."

- **The bandwidth to be more proactive and strategic, instead of reactive.** Interviewees said their organizations' improved abilities to take proactive approaches to compliance are valuable because their employees now have the time and the tools to do so. With the process efficiencies enabled by Microsoft 365 E5 Compliance, the interviewees' organizations were able to reallocate staff time from repetitive and often reactive manual processes to higher-level and more strategic initiatives.

  The director of IT at the healthcare organization said: "Getting that time back allows [the IT staff to] get ahead of the curve by giving [staff members] the ability to do other things. Maybe they're able to get to inquiries faster if there's anything pending. Or they're able to educate folks who aren't in the risk space about the importance of managing risk. So, [Microsoft 365 E5 Compliance allows IT staff to be] more of a resource with the time to have conversations with people as needed."

- **Greater ease and consistency in compliance reporting.** The VP of IT and cybersecurity at the information services company said: "When our individual businesses each did their own reporting, there was a lot of subjectivity. Now, we have a central audit team handling reporting with integrated tools and information. Reporting takes much less time, and the reports are standardized."

- **Improved ability to anticipate and respond to compliance requirements of international expansion.** When the interviewees' organizations expanded into additional countries, they used the frameworks and tools of Microsoft 365 E5 Compliance to determine what efforts would be needed around country-specific regulations and compliance. The CISO at the professional services firm said: "[Microsoft 365 E5 Compliance] provides visibility to where we're growing and the efforts we'll need to undertake there, and it simplifies those efforts because we do them using a single system."

- **Shorter turnround times on information requests and legal processes.** The interviewees' organizations gained the ability to respond to internal or external requests for information much more quickly because they now have access to an integrated set of tools and all the pertinent information in one place. For example: Requiring less manual effort for e-discovery enabled the organizations to move faster on legal processes, which interviewees said gave them a stronger position.

  The CISO at the professional services firm said: "Our shorter time-to-information is a big deal. Giving our legal department more time by providing information faster helps them get to better decisions faster. Imagine dealing with an incident and not having the information you need for a day or two versus having that information in an hour."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Microsoft 365 E5 Compliance and later realize additional uses and business opportunities, including:

- **Leveraging existing capabilities more fully.** Microsoft 365 E5 Compliance has a broad range of capabilities that customers may deploy incrementally over time.

- **Using new capabilities as they are introduced.** A senior director of IT security at the professional services firm said: "We get the benefit of Microsoft continuing to evolve their platform, without us doing anything."

"We will definitely have further cost savings and optimization as we leverage more of the existing functionality. And Microsoft continues to add new features."

Head of cybersecurity, natural resources

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

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	Microsoft fees	$396,000	$1,584,000	$1,584,000	$1,584,000	$5,148,000	$4,335,174
Ftr	Internal labor for implementation, management, optimization, and support	$528,165	$142,912	$142,912	$142,912	$956,901	$883,566
	Total costs (risk-adjusted)	$924,165	$1,726,912	$1,726,912	$1,726,912	$6,104,901	$5,218,740

MICROSOFT FEES

Evidence and data. Microsoft fees reflect annual subscription costs for Microsoft 365 E5 Compliance. The subscription fee includes a standard level of support.

Since subscription costs are determined by customer-specific factors, consult with Microsoft for likely costs specific to your organization when conducting your own analysis. Your organization’s subscription fees may differ from the composite organization’s fees.

Modeling and assumptions. For the composite organization, Forrester models Microsoft fees at $12 per user per month. Initial costs reflect fees paid during implementation.

Risks. Microsoft fees will vary based on:

- The purchase structure (e.g., whether an organization purchases individual Compliance modules or the full Compliance suite, or if it gains access to Compliance as part of an overall Microsoft 365 E5 purchase or an upgrade from Microsoft 365 E3).
- The number of licensed users.

Results. Because these factors are known for the fees described here, Forrester did not risk-adjust this cost upward, yielding a three-year total PV (discounted at 10%) of $4,335,174.

Microsoft Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Number of employees	Composite	11,000	11,000	11,000	11,000
E2	Monthly per employee subscription fee	Microsoft	$12	$12	$12	$12
E3	Number of months paid	Interviews	3	12	12	12
Et	Microsoft fees	E1*E2	$396,000	$1,584,000	$1,584,000	$1,584,000
	Risk adjustment	0%				
Etr	Microsoft fees (risk-adjusted)		$396,000	$1,584,000	$1,584,000	$1,584,000
	Three-year total: $5,148,000			**Three-year present value: $4,335,174**		

INTERNAL LABOR FOR IMPLEMENTATION, MANAGEMENT, OPTIMIZATION, AND SUPPORT

Evidence and data. The interviewees said their organizations typically implemented Microsoft 365 E5 Compliance using internal resources from their IT teams and other functions such as risk, security, HR, and legal, supported by informal assistance from Microsoft.

Implementation usually included 30 to 60 minutes of training for all employees about the information protection and governance capabilities and several days of training for power users (individuals from varied functions who work more extensively with Microsoft 365 E5 Compliance).

Interviewees reported that Microsoft 365 E5 Compliance requires minimal technical support on an ongoing basis. For the composite organization, a team of power users continues to expand the organization’s use of existing capabilities and leverages new capabilities as they are released.

Modeling and assumptions. For the composite organization, Forrester assumes that initial costs include:

- A total of 2,500 hours of staff time for implementation.
- 20 hours of training for each of its 40 power users.
- 45 minutes of training for each of its 11,000 employees.

For the composite organization, Forrester assumes that ongoing annual costs include:

- A total of 2,000 hours of staff time for management, optimization, and support.
- 6 hours of training for each of its 40 power users.

Risks. The initial and ongoing internal labor costs will vary based on:

- The scope and complexity of the implementation.
- The experience and capabilities of the staff.
- The number of individuals trained.
- The extent to which an organization continues to expand and modify its use of the full capabilities of Microsoft 365 E5 Compliance.
- Prevailing local compensation rates.

- **Results.** To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $883,566.

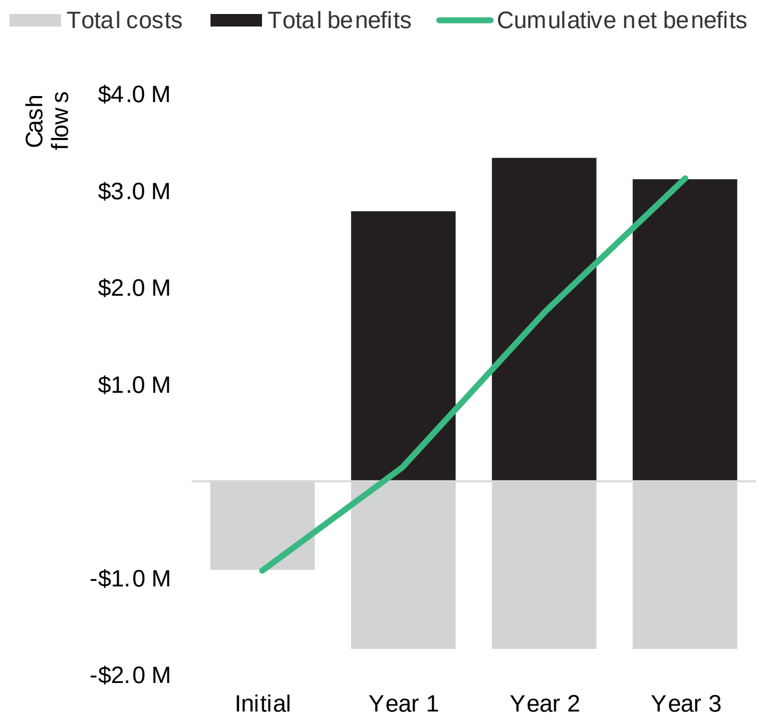
Internal Labor For Implementation, Management, Optimization, And Support

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Staff time required for implementation and subsequent management, optimization, and support (combined total hours)	Interviews	2,500	2,000	2,000	2,000
F2	Average hourly, fully burdened compensation per implementation staff member	Assumption	$58	$58	$58	$58
F3	Number of power users trained	Interviews	40	40	40	40
F4	Training time per power user (hours)	Interviews	20	6	6	6
F5	Average hourly, fully burdened compensation per power user	Assumption	$58	$58	$58	$58
F6	Number of employees trained	Composite	11,000	0	0	0
F7	Training time per employee (hours)	Interviews	0.75	0	0	0
F8	Average hourly, fully burdened compensation per employee	Assumption	$35	$0	$0	$0
Ft	Internal labor for implementation, management, optimization, and support	(F1*F2)+(F3*F4*F5)+ (F6*F7*F8)	$480,150	$129,920	$129,920	$129,920
	Risk adjustment	↑10%				
Ftr	Internal labor for implementation, management, optimization, and support (risk-adjusted)		$528,165	$142,912	$142,912	$142,912
	Three-year total: $956,901		Three-year present value: $883,566			

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	($924,165)	($1,726,912)	($1,726,912)	($1,726,912)	($6,104,901)	($5,218,740)
Total benefits	$0	$2,784,689	$3,338,109	$3,114,599	$9,237,397	$7,630,348
Net benefits	($924,165)	$1,057,777	$1,611,197	$1,387,687	$3,132,496	$2,411,608
ROI						46%
Payback period (months)						11.0 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."

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.

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.

Appendix B: Endnotes

[1] Source: Ben Wolford, “What are the GDPR fines?,” GDPR.eu (https://gdpr.eu/fines/).
[2] Source: “Cost of a Data Breach Report 2020,” Ponemon Institute, April 2020.
[3] Source: “Cost of a Data Breach Report 2019,” Ponemon Institute, April 2019.

FORRESTER®