

White Paper

Microsoft Azure Is Helping Organizations Manage Regulatory Challenges More Effectively

Sponsored by: Microsoft

Ryan O'Leary
May 2019

Harsh Singh

EXECUTIVE SUMMARY

As regulations burdening enterprises continue to increase, enterprises are looking for more efficient and comprehensive ways to manage risk and compliance. While many solutions have emerged to tackle the increased regulatory burden, they also add onto existing infrastructure instead of being encompassed in it. Governance, risk, and compliance (GRC) tools that are embedded in a public cloud service may provide added benefits not available elsewhere.

IDC interviewed organizations that are using Microsoft Azure as a platform to optimize their regulatory compliance initiatives. Special emphasis was placed on survey data derived from government, healthcare, and financial sectors. Based on the data gathered, IDC found that these organizations are realizing significant benefits by leveraging Azure capabilities to make their regulatory and compliance efforts more effective while doing so in a secure and cost-effective manner. According to IDC calculations, the organizations surveyed will realize annual benefits worth \$4.29 million per organization by:

- Increasing the efficiency and productivity of managing compliance tools, the compliance environment, and auditing
- Reducing the costs of compliance-related penalties
- Improved agility in responding to new and ever-changing national and international regulations
- Enhancing the overall productivity of auditing and compliance teams as well as IT support
- Reducing the incidence of unplanned downtime and minimizing the use of help desk

Business Value Highlights

- 465% ROI
- 6 months to payback
- 24% more productive regulatory compliance teams
- 39% improved agility in responding to new regulations
- 35% lower costs of compliance-related penalties
- 47% reduction in unplanned downtime
- 27% more efficient auditing staff
- 27% more efficient IT compliance environment management teams

SITUATION OVERVIEW

In years past, only select industries, such as finance, health, and manufacturing, faced heavy regulation, but with the onset of broader privacy regulation, every industry is now facing an increased regulatory burden. Regulation is pervasive as more regulations are passed, rarely if ever are they repealed. Globally, there are thousands of regulations governing multiple aspects of business, and compliance seldom increases revenue – it only incurs cost. However, the risk of noncompliance can be very significant, with some regulations threatening fines of 4% of total revenue. Fines and sanctions that were once a mere setback could now be the end of a business.

In addition to regulation, the enterprise view of risk has matured and expanded beyond just complying with regulations. Data breaches and security incidents continue to be regular occurrences, and protecting against reputational and business harm they can cause is critical. Attacks can come from both internal and external sources making strong security controls paramount in any GRC program.

A natural extension of the current regulatory and risk climate is that enterprises must now look for ways to efficiently and inexpensively manage those complex obligations. Unsurprisingly, the market has rushed to create solutions. While solutions vary in size, scope, and design, they often take the form of GRC platforms with multiple modules specializing in specific tasks. Others are point solutions that integrate directly into a security environment to automate and support complex tasks with security-centric controls. Most of these solutions overlay on top of an organization's infrastructure instead of being imbedded in it. Perhaps, building the GRC solution directly into the infrastructure may be an efficient way to attack the problem of adhering to complex compliance requirements in the cloud. A built-in GRC solution would have the added benefit of the cloud service provider as the data processor shares risk with the organization it serviced.

AZURE TOOLS FOR GOVERNANCE, RISK, AND COMPLIANCE

Microsoft has built its compliance solution directly into the Azure cloud service. Azure has a portfolio of over 90 compliance offerings such as certifications for standards like HIPAA, FedRAMP, and ISO/IEC 27018, many of which are built with the specific needs of heavily regulated industries in mind.

On top of the regulatory compliance frameworks built into Azure, Microsoft also provides a set of services to help implement compliance, including:

- Azure Blueprints helps customers build Azure applications that are secure and comply with many regulations, including the GDPR and HIPAA, both internally and externally.
- Azure regulatory compliance dashboard provides insight into compliance posture for a set of supported standards and regulations, based on continuous assessments of the Azure environment.
- Azure Policy helps define and enforce policies that help the Azure environment become compliant with internal policies and external regulations.

The Azure compliance toolset further builds in control-mapping capabilities, workflow management tools, and audit functionality.

In addition to compliance tools, the Azure infrastructure combats security risks with stringent digital and physical security controls. Azure has highly secure datacenters with robust physical security measures. Microsoft deploys 3,500+ security professionals who constantly monitor and improve Azure.

As an additional security measure, Microsoft ensures that access is accorded to the bare minimum of administrators needed to complete a task.

THE BUSINESS VALUE OF USING AZURE AS A COMPLIANCE PLATFORM

Study Demographics

IDC conducted research that explores the value and benefits for organizations in the United States that are using Azure to support their regulatory compliance. The study included 12 interviews that fielded quantitative and qualitative questions about the impact of Azure compliance on their IT infrastructure and compliance operations, businesses, and costs.

Table 1 presents the demographics for the organizations surveyed, which averaged an employee base of 12,000+ people. Most of these organizations were supported by an IT staff of, on average, 170 employees running about 50 business applications. The number of regulatory compliance staff members was 51. (Note: All numbers cited represent averages not medians.) The vertical industries represented include the government, healthcare, and financial services sectors. These sectors were examined individually in terms of specific benefits that organizations experienced.

TABLE 1

Firmographics of Surveyed Organizations

	Average	Median
Number of employees	12,153	3,393
Number of IT staff	170	177
Number of regulatory compliance staff	51	24
Number of employees using IT services	12,095	3,393
Number of external users/customers	255,047	5,000
Number of business applications	50	25
Industries	Government (4), healthcare (4), and financial services (4)	

n = 12

Source: IDC, 2019

Organizational Usage of Azure for Compliance Workloads

Study participants described company usage patterns for Azure as well as a snapshot of the overall IT and business environments that Azure supported. They also discussed both the value proposition and rationale behind their choice of Azure. Customers cited increased digitization as an important factor as well as the need for more robust security features. Ease of integration and use were also considered

important criteria as was the brand value that Microsoft brought to the table with a trusted and robust mix of compliance solutions. Study participants made specific observations about these benefits:

- **A more digitalized regulatory environment requires better security:** "Our regulatory compliance is changing now because ... a lot more is now digital, such as exchanging data with the appropriate regulatory agency. Moving forward, I think there will be a push for more data security because everything is becoming digitized. We use Azure for compliance to make sure we're covered from an IT security standpoint."
- **Microsoft is a trusted vendor:** "We have always worked with Microsoft as an operating platform, so we knew and trusted the company. Once we saw how much easier it would be to generate reports, we moved toward Azure."
- **Azure offers a depth of compliance:** "Microsoft has the most globally accepted compliance portfolio. It maintains the largest compliance portfolio, by far, of any cloud-based software solution."
- **Azure provides strong security and support:** "We decided to use Azure to manage our compliance workloads because it had a good track record of being secure ... There were additional deciding factors such as ease of integration with our existing legacy systems, customer support, scalability, cost-effectiveness, and ease of use."
- **Azure is a good fit with existing regulatory workloads:** "Regulatory compliant workloads are easier to deploy with Azure ... Azure for compliance workloads does not require any additional customization. Even though we have a multiple cloud environment, Azure is meeting our requirements perfectly."

Table 2 provides data on the IT environments that characterized surveyed companies as well as specifics on how Azure was being used to manage compliance. Additional usage patterns are presented in Table 2.

TABLE 2

Azure Usage for Compliance

	Average	Median
Number of months using Azure	22	20
Number of branches/sites	39	35
Number of compliance staff	92	37
Number of business applications	19	10
Number of Azure instances	15	8
Number of terabytes, Azure environment	79.2	10.5
Percentage of total revenue	67	50

Source: IDC, 2019

Business Value Analysis

Interviewed organizations explained that they have leveraged Azure as a compliance platform to fundamentally improve key aspects of their compliance operations. Based on the data gathered, IDC found that the organizations studied are realizing significant benefits by leveraging Azure capabilities to make their domestic and international regulatory and compliance efforts more effective in a cost-effective, secure manner. Microsoft's reputation and excellent support capabilities were also cited. As a result, study participants can maintain compliance requirements, conduct more effective audits, and better avoid penalties and fines associated with noncompliance.

Study participants discussed how Azure helps them achieve these benefits in compliance management:

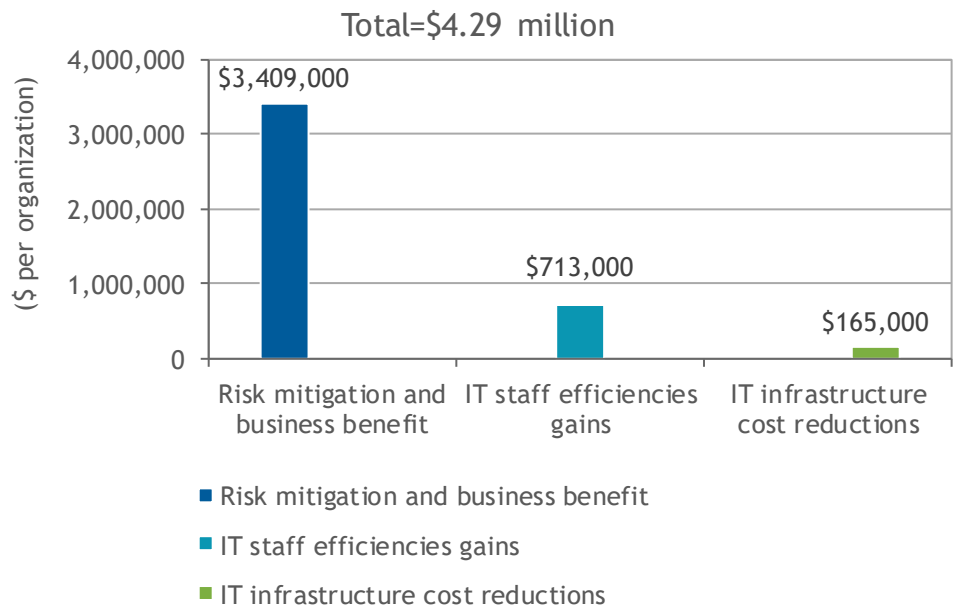
- **Improved benefits across the board:** "We are seeing a lot of different benefits. Azure compliance is very fast across the board and is more agile. We now have global reach with it. Disaster recovery is probably paramount. We are getting exceptional customer support. Microsoft has dedicated area experts to answer questions. Scalability is good as is the cost-effectiveness and long-term return on investment (ROI). Enterprise security is cutting edge ... and we are very compliant ... our compliance rating is up."
- **Depth of offerings:** "Azure compliance had the best database and a wide range of service offerings. Their services draw on AI and machine learning. It is a full service so we don't have to work with a lot of companies ... we can do a lot of things from one source. Azure is more economical and has made us more efficient in terms of how fast we get things done."
- **Excellent security, customer support, and payment structure:** "Security is number 1. We also care a lot about compliance, and Microsoft had the best and most complete compliance offering on the cloud. They also offer a wide range of IT support including automatic patches and upgrades. Another reason is they are integrated with existing Microsoft licenses. We pay for what we use and can scale up or down accordingly."

As shown in Figure 1, IDC quantifies the value over five years that study participants are achieving through their use of Azure for compliance as an average of \$4.29 million per year per organization in the following areas:

- **Risk mitigation and business benefits:** Compliance efforts were more effective, and both IT and compliance teams are more productive. IDC calculates the value of higher revenue, increased productivity, and lower business costs at an annual average of \$3.4 million per organization.
- **IT staff productivity gains:** Azure enabled more efficient and productive compliance tool management and compliance environment management. As a result of this benefit, IDC calculates that customers will realize annual value of \$713,000.
- **IT infrastructure cost reductions:** Azure offered the benefit of lower infrastructure costs. IDC calculates that study participants will realize an annual value of \$165,000.

FIGURE 1

Average Annual Benefits per Organization



Source: IDC, 2019

Improved Regulatory Compliance

Study participants reported that use of Azure as a compliance platform helped them carry out their day-to-day compliance responsibilities more effectively. Azure helped them better manage spikes in the workload, enabled faster access to and analysis of data during audits, and reduced exposure to risk based on the strong internal controls of Azure. Other participants discussed the benefit of being able to save time and thereby keep costs in check. Study participants commented on these benefits:

- **Better workload management and reduced risk:** "We are able to stay on top of what we are doing, and we can now handle growth or spikes in the workload. Azure has lessened our exposure to risk because of its strong internal controls."
- **Increased audit efficiency:** "Azure has absolutely helped with audits. For example, it allows us to have much better and faster access to our data, and faster analysis of that data for our audits. Compliance teams save time as a result."
- **State-of-the-art security:** "Azure has lessened compliance risk exposure because its ... security systems are state of the art. There is less chance of any kind of data being compromised through intrusion."

Table 3 shows regulatory compliance staff impacts as calculated by IDC. As shown, FTEs were reduced, representing a 24% improvement. This benefit translated into cost savings for companies using Azure compliance amounting to \$880,121 on an annual basis.

TABLE 3

Regulatory Compliance Staff Impact

	Before Azure	With Azure	Difference	Change (%)
Regulatory compliance staff (FTEs before/after)	52.1	39.6	12.6	24
Staff time cost per year (\$)	3,649,189	2,769,068	880,121	24

Source: IDC, 2019

Figure 2 presents compliance staff efficiencies enabled by using Azure for compliance in the course of their work. For example, assessing compliance was 20% more efficient after deploying Azure, while compliance and remediation reporting were each 14% more efficient.

FIGURE 2

Compliance Staff Time Efficiencies

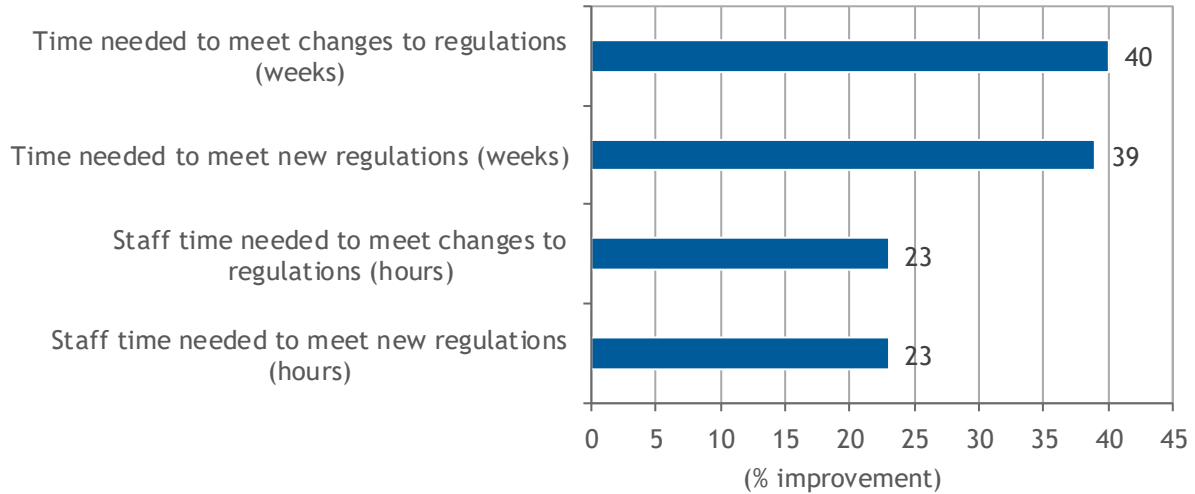


Source: IDC, 2019

IDC quantified the regulatory agility of organizations studied – that is, their ability to respond to requirements and timelines in the compliance process. Especially noteworthy is the reduction by 40% of the time needed to meet changes to regulations, and the time required to comply with new regulations was improved by 39%. Staff spent 23% less time addressing regulatory change and new regulations (see Figure 3).

FIGURE 3

Regulation Agility Benefits



Source: IDC, 2019

Table 4 shows FTE-based staff impacts for the auditing function. As shown, both staff FTEs and staff time cost per year showed a 27% improvement. Annualized staff time costs were significant and calculated at \$244,882.

TABLE 4

Auditing Staff Impact

	Before Azure	With Azure	Difference	Change (%)
Auditing staff (FTEs before/after)	12.9	9.4	3.5	27
Staff time cost per year (\$)	903,875	658,993	244,882	27

Source: IDC, 2019

Impact on Risk Mitigation

As a result of using Azure for compliance, study participants experienced a reduction in unplanned downtime and an increase in business productivity. Table 5 shows that outages were reduced almost 50% as were the number of hours staff spent addressing them. Especially noteworthy, this yielded a savings of \$1,287,132, representing a 47% improvement.

TABLE 5

Unplanned Downtime Impacts

	Before Azure	With Azure	Difference	Change (%)
Frequency of unplanned downtime per year	19.5	10.2	9.4	48
Mean time to repair (MTTR)	3.4	2.0	1.5	43
Hours lost per user	6.1	3.3	2.9	47
FTE productivity impact	39.4	21.1	18.4	47
Cost of unplanned downtime, per year (\$)	2,761,124	1,473,991	1,287,132	47

Source: IDC, 2019

As Table 6 illustrates, the positive effects of reduced unplanned downtime extended to help desk operations for the organizations surveyed, which cut help desk calls from 176 per year to 132, a decrease of 25%. This also resulted in an annual staff costs savings of almost \$270,000, a one-third improvement.

TABLE 6

Help Desk Impacts

	Before Azure	With Azure	Difference	Change (%)
Calls per year	176	132	45	25
Mean time to repair	4.3	3.3	1.0	24
Help desk FTEs productivity impact	8.0	5.3	2.7	34
Staff time cost per year (\$)	796,941	528,539	268,402	34

Source: IDC, 2019

Increased Efficiencies for IT Operations

Study participants reported that IT teams also benefited from having the robust and efficient platform of Azure for compliance procedures. Table 7 shows improvement in productivity for managing both compliance tools (such as the Azure regulatory compliance dashboard and Azure Policy) and the compliance environment. IDC calculations for compliance tool management impacts are listed in Table 7. As shown, both FTEs involved in management of compliance tools and the amount of associated staff time costs saved in that process showed a 25% improvement.

TABLE 7

IT Compliance Management Impact

	Before Azure	With Azure	Difference	Percentage Change
Management of compliance tool (FTEs before/after)	7.1	5.3	1.8	25
Staff time cost per year (\$)	711,873	530,444	181,429	25
Management of compliance environment (FTEs before/after)	4.5	3.2	1.2	27
Staff time cost per year (\$)	445,942	323,855	122,087	27

Source: IDC, 2019

More Cost-Effective Infrastructure and Operations

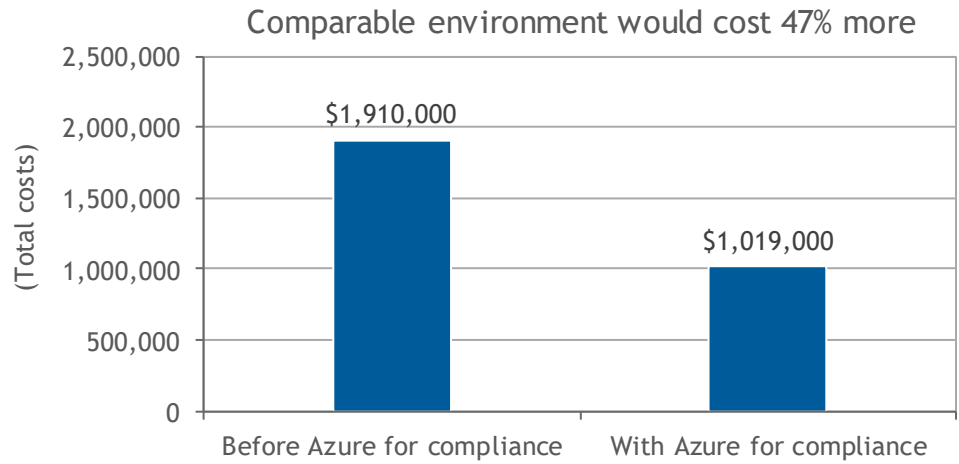
For study participants, using Azure as a compliance platform represented a more cost-effective solution than other commercial alternatives they considered. The associated cost savings included having a solution that scales to varying work requirements quickly, reductions in server hardware based on the use of cloud-based resources, and licensing cost savings. Study participants spoke in detail about these benefits:

- **More cost effective:** "One of the most significant benefits is long-term return on investment ... When we did a cost-benefit analysis, Azure was found to be 15-20% more cost effective."
- **Reductions in servers and hypervisors:** "We reduced half of our servers because our regulatory compliant applications no longer needed physical servers to support them. We were able to drop about 40 hypervisors as well because of Azure."
- **Greater infrastructure density:** "We reduced some of our equipment and licenses. I would say we avoided refreshing \$50,000 worth of equipment such as servers and some ancillary equipment."

Figure 4 shows IT infrastructure savings in deploying Azure for compliance with the cost of an alternative solution. As shown, a comparable infrastructure would almost double the cost over a five-year period compared with Azure.

FIGURE 4

Five-Year IT Infrastructure Costs

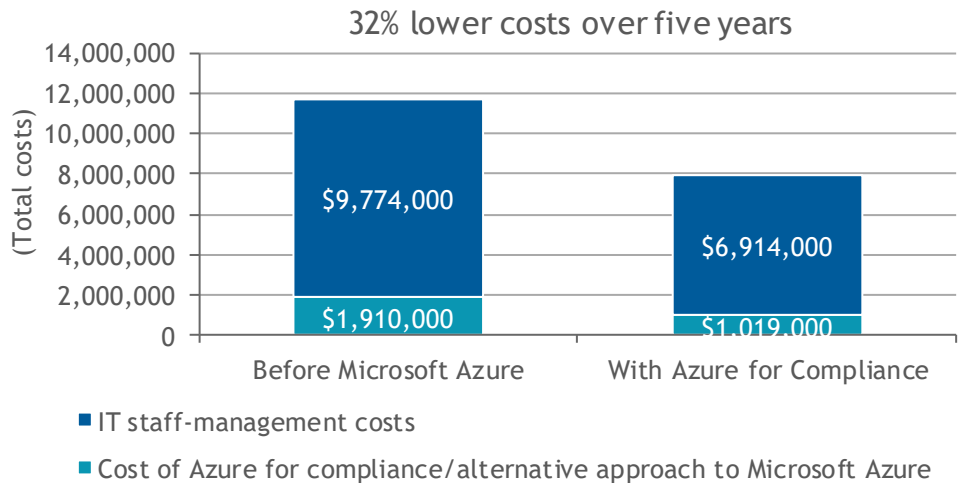


Source: IDC, 2019

Cost savings also were evident in operational costs. Figure 5 compares the cost of operations before and after deploying Azure. IDC used two evaluation criteria to these calculations: IT staff management costs and the cost to implement Azure compared with the cost of an alternative solution. As shown in the Figure 5, operational costs when organizations deployed Azure were 32% lower over a five-year period.

FIGURE 5

Five-Year Cost of Operations



Source: IDC, 2019

Differentiated Value of Azure for Compliance: Government

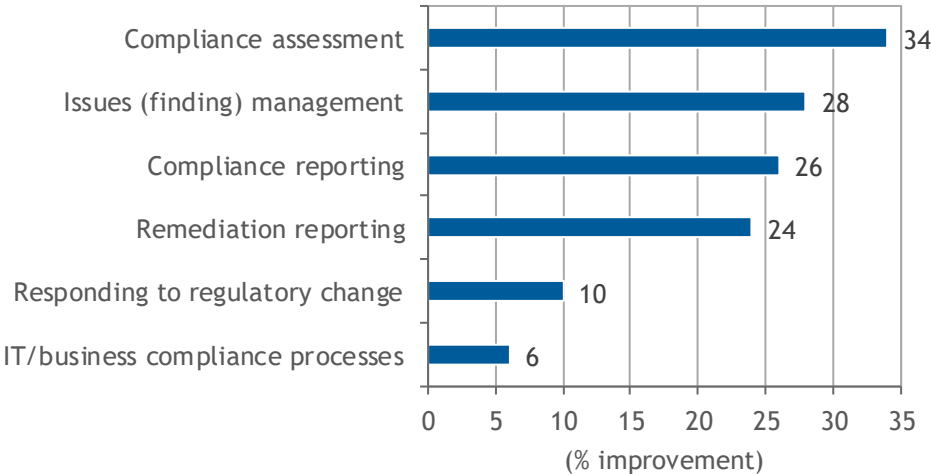
Government agencies represented a key vertical that IDC surveyed. These agencies reported a number of benefits as the result of deploying Azure to manage compliance. These included having a set of comprehensive tools for compliance management with good visibility into functions and ease of use, as well as the ability of the platform to flexibly address compliance requirements while offering analytics capabilities. Study participants spoke in detail about these benefits:

- Well suited for government workloads:** "Azure is a portfolio of solutions for full life-cycle management for everything we do. We found that different case studies for others who used it made sense for us and our requirements because Azure is able to support both for-profit and nonprofit organizations. We needed a worldwide, trustworthy, first line of defense and Azure has provided that. It is well integrated and offers the most comprehensive tools for management in the industry and the most secure system. We are able to much better execute our mission thanks to the capabilities of Azure compliance and the specialized support provided."
- Improved data analysis and protection:** "Azure allows us to use analysis as well as the data protection we need to protect people's information. Without it, we could not do our work – people wouldn't trust us. We get actionable insights that is necessary in the evolving areas we work in. We get compliance support but also are able to do other things with the data we have. It is more than just a compliance investment."
- Ease of management:** "A key government requirement is to make sure that certain ports aren't open. Azure made it very easy to see which ports are available so we could shut those down, if needed. Before, we would have to research it by going into our internal servers to try and find out what was going on. It was very black boxy. Now there is more visibility."

Figure 6 quantifies and breaks down the benefits associated with saving staff time for government organizations. For example, assessing compliance is 34% more efficient when deploying Azure, while compliance reporting is 26% more efficient.

FIGURE 6

Compliance Staff Time Savings – Government



Source: IDC, 2019

Differentiated Value of Azure for Compliance: Financial Organizations

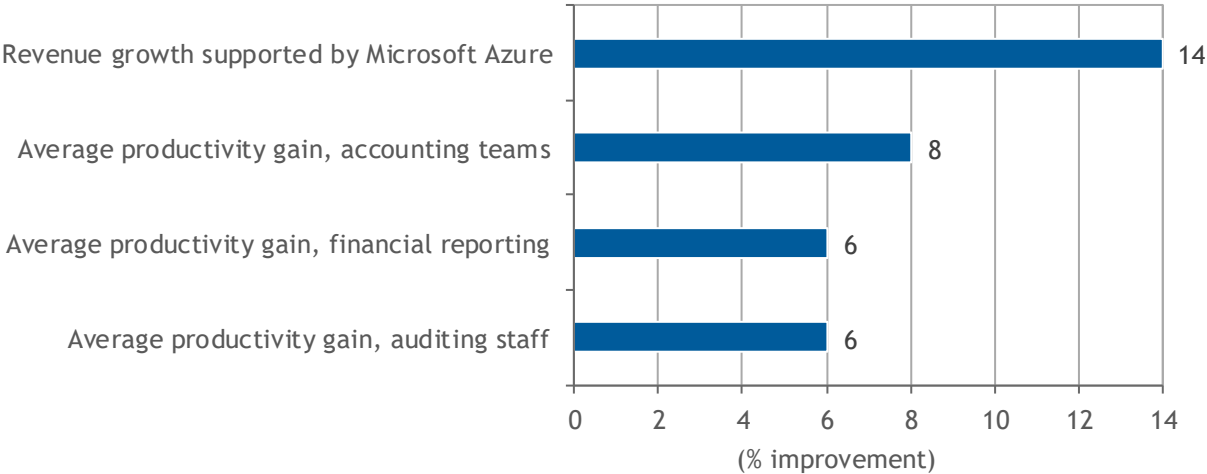
Financial organizations reported a number of key benefits after deploying Azure as their compliance platform. Study participants cited robust security features that manage identity and administration, protect proprietary information and reduction of risk, and the ability to handle the increasing demands of international regulation as the key benefits from Azure. Study participants spoke in detail about these benefits:

- **Keeps pace with United States and international regulations:** "What's important to us is being current with all the regulations. SEC regulations are what we are most concerned with, but we're seeing growth in international regulations. It's the organization, streamlined access, and automation of Azure that has had the most positive impact for us."
- **Financial data is more secure:** "Our biggest challenge is ensuring that financial data is secure and not compromised. This sounds simple but we are constantly responding to new threats. Azure secures our network and manages identity and administration. Azure's unified security management keeps everything secret, protecting proprietary information. We are also able to do financial reporting on time and accurately."
- **Offers security and a broad solution:** "The main benefit is security and having a robust and broad solution from a single vendor. We are confident that Microsoft will be our platform for the foreseeable future."
- **Reduces risk of financial penalties:** "Azure for compliance is phenomenal when it comes to reducing our exposure to risk. This has been great because we have less worry about not following policies and regulations. It has helped us develop best practices, avoiding financial losses or penalties."

Figure 7 quantifies and breaks down key benefits to financial organizations. For example, using Azure as their compliance solution yielded a 14% growth in revenue and an 8% improvement in the productivity of accounting teams. Additional metrics are shown in Figure 7.

FIGURE 7

Key Finance Benefits



Source: IDC, 2019

Differentiated Value of Azure for Compliance: Healthcare

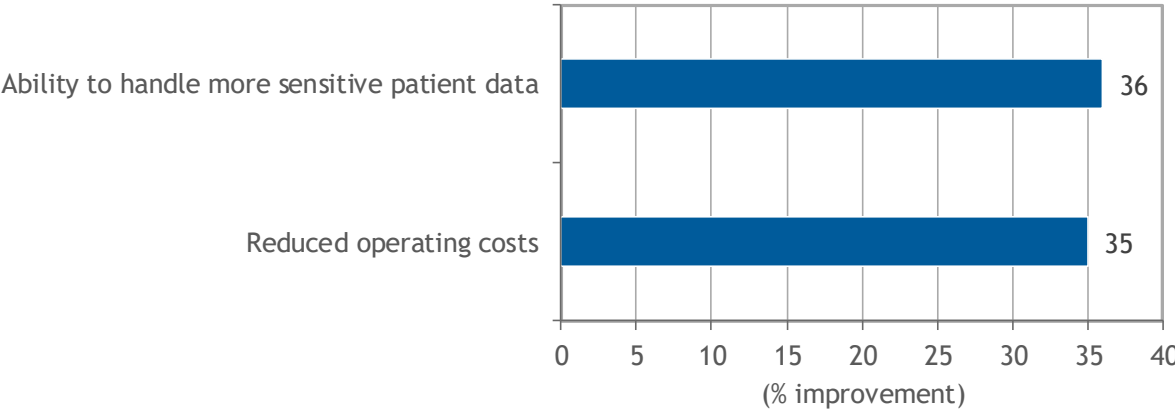
Healthcare organizations reported benefits as the result of deploying Azure as their compliance platform. Strong HIPAA and HITECH compliance was cited as an important factor especially because those features were not available with a previous solution. Organizations also responded positively to such benefits as the ability to streamline the transmission of HIPAA data, effective report creation, and the ability to easily modify and customize reports – a benefit appreciated in particular by senior management. Study participants spoke in detail about these benefits:

- **Manages various data sources seamlessly:** "One of the challenges we face is importing data from other systems. We are big users of the EPIC electronic medical records system and it is a huge work in progress. We have different environments and have the challenges with transferring data from one environment to another."
- **Positioned to respond to existing and new regulations:** "The most important thing is having a secure, encrypted, auditable database that can reliably process our workload and that helps us conform to HIPAA and HITECH. Azure compliance also puts us in a position to deal with future regulations."
- **Provides streamlined reporting capabilities:** "Azure compliance has a big impact in terms of streamlining the processes of sending data to HIPAA. It has also played a big role in the report creation process since we typically get requests from various departments to produce data reports that involve a series of processes."
- **Easier report generation:** "With Azure we can modify and customize different reports at will. Senior management likes this, and it led them to have us evaluate Azure more fully. Once we saw how much easier it would be to generate reports, we moved to Azure."
- **Supports strong HIPAA compliance:** "We were looking to go to the cloud a few years ago. It was a choice between Microsoft and a competitor's offerings. At the time the competitor's database product was not guaranteed to be HIPAA compliant. Plus, we work a lot with Microsoft and are confident in them as a supplier."

Figure 8 represents the key benefits to healthcare organizations: their ability to handle more sensitive patient data showed a 36% improvement, and operating costs were reduced by a little over a third.

FIGURE 8

Key Healthcare Benefits



Source: IDC, 2019

Impact of Azure Blueprints

About half of the organizations surveyed also were using Azure Blueprints. Companies reported a number of benefits including better visibility into and remediation of threats and vulnerabilities through monitoring and analytics that are always available. They also reported appreciation for the guidance documents, accreditation, and automation scripts for hosting web applications. In addition, study participants cited its capabilities as a full-service platform offering auditing and features such as activity and diagnostic logs. Study participants spoke in detail about these benefits:

- **Full-service platform:** "The architecture is already set up and is very sophisticated (e.g., different app services, load balancers, and the database are all set up). We don't have to spend a lot of time on architecture. Other benefits are the resource manager, security management, logging and auditing, activity logs, and diagnostic logs. It is a great resource for support of our ongoing compliance requirements."
- **Globally available PaaS with many built-in features:** "Azure Blueprints have everything as a PaaS (e.g., guidance documents and applications, accreditation and compliance, and automation scripts for hosting web applications). Blueprints give us an entire environment and everything is handled very professionally. They have worldwide data security standards and a strong platform worldwide."
- **Better visibility into threats and vulnerabilities:** "The benefits of Azure Blueprints are security management in particular with 24 x 7 monitoring. It fixes vulnerabilities before they can be exploited. It's a much more simple threat response solution and works more quickly than what we have had in the past. We can see attacks through analytics. The best part of it are the policies that ensure we are up to date and compliant with security standards."

ROI Analysis

Table 8 presents IDC's analysis of the benefits and costs related to the use by surveyed organizations of Azure as a compliance solution. IDC projects that these organizations will, over five years, realize discounted benefits of over \$13 million per organization (or about \$110,000 per 100 internal users). When compared against a discounted investment of almost \$2.4 million per organization, these organizations will see an ROI of 465% and a breakeven on their investment in six months.

TABLE 8

Five-Year ROI Analysis

	Total	Per 100 Users
Benefit (\$)	13,303,134	109,993
Investment (\$)	2,353,557	19,460
Net present value (NPV) (\$)	10,949,576	90,533
ROI (NPV/investment)	465%	465%
Payback (months)	6.0	6.0
Discount factor	12%	12%

Source: IDC, 2019

CHALLENGES AND OPPORTUNITIES

Microsoft is challenged, of course, by other public cloud service providers competing for a finite number of customers. Microsoft, which already has a deep compliance offering, will need to continue to stay on top of the latest regulations and build them into its services. Microsoft is not only competing with cloud service providers but in the compliance realm as well. There are many solutions that can automate IT security and compliance controls within public cloud services. To keep its market share, Microsoft will need to continue to ensure that its built-in security controls are as good if not better than those available from third parties.

IT security and compliance is just one part of the GRC universe. Azure and its Office 365 suite contain a large portion of the data that enterprises are trying to ensure is compliant with internal policies as well as external regulations. Microsoft has a real opportunity to create a GRC platform that is seamlessly integrated with Azure to compete with the other GRC platforms that only take data feeds or other imports from Azure. If Microsoft could create an internal GRC platform that manages an enterprise's entire compliance program, it could change the GRC landscape.

On the security front, Microsoft has the challenge of increasingly deceptive and sophisticated bad actors who will stop at nothing to gain access to Azure data. Microsoft will need to continue to invest heavily in its security program including talent development because of the shortage of experienced security professionals on the job market. Microsoft will further need to anticipate new technologies that may arise that could put their services at risk of a security incident.

SUMMARY AND CONCLUSION

The regulatory framework affecting businesses continues to grow in complexity with no signs of slowing. Enterprises are under pressure to as cheaply as possible effectively manage this risk. If the risk is not managed effectively, there could be drastic consequences for businesses. Consequently, enterprises have begun deploying software solutions to manage the compliance and risk process.

Most solutions aimed at tackling internal and external GRC activities are deployed as software that integrates on top of infrastructure. The challenge of integrating a GRC solution into infrastructure can hinder the compliance activities of businesses. Responding to those challenges, Microsoft offers compliance tools built directly into its Azure product. The compliance tools provided by Microsoft emphasizes breadth, with compliance tools for over 90 regulations, and security, with over 3,500 security professionals. Microsoft's solution further provides analytics dashboards and automated policy management right in the cloud infrastructure.

As demonstrated in this white paper, the result for Microsoft's customers is business value that is derived from efficient risk and compliance features that permeate their enterprise systems. That business value is exhibited through increased compliance staff productivity, a decrease in network downtime, and increased security and risk posture.

As organizations continue to strive for efficient and comprehensive GRC operations and protect their organizations better and cheaper, these organizations realize that building compliance tools into their systems can easily achieve these objectives. Microsoft is well positioned to provide value and protect organization's data and business from their core.

APPENDIX

Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of Azure for their regulatory compliant workloads as the foundation for the model. Based on interviews with organizations using Azure, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Azure.** In this study, the benefits included staff time savings and productivity benefits and operational cost reductions.
2. **Created a complete investment (five-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Azure and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Azure reports over a five-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded \$100,000 per year salary for IT staff members, and an average fully loaded salary of \$70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the five-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.

