Digital Risk, Compliance, and Data Centricity

*The Value of Centralization in a Distributed World*

TABLE OF CONTENTS

1 Summary
2 What is Driving Strategy Today?
3 Causes and Effects
4 What To Do In Response?
5 Discussion and Conclusion
6 About the Research
7 Acknowledgements
8 About Microsoft
9 About Jon Collins
10 About GigaOm
11 Copyright
1. Summary

This report examines the current state of digital governance, risk, and compliance within enterprise companies—an area that has recently seen dramatic shifts in policy, strategy, and working practices. We reached out to enterprises across a variety of industries to gauge their efforts to combat these challenges.

"We have seen a rapid acceleration of our customers’ digital transformation due to the increased need to support work from anywhere. These changes in how people work have introduced new risk and the need to protect and govern data in different ways. A holistic approach to risk management is critical to address security and compliance properly across the environment. We are working closely with our customers and partners to meet these challenges in an era of rapid change."

Alym Rayani, GM, Microsoft

The research, based on over 300 survey respondents in the US and Europe, and supported by interviews with leading consulting and services firms, shows:

- Digital transformation is the number one priority affecting organizations today, both despite and because of recent events. Alongside privacy and regulation, consumer needs and reputational risk are significant factors driving activity.

- The fast-moving regulatory landscape and continued, rapid data growth conspire to create significant risk and compliance challenges. External hacking and cloud-based data breaches are also seen as a source of risk.

- The journey to the cloud is one way organizations are accelerating the movement of unstructured data (e.g. documents, spreadsheets or email and chats) to cloud-based, centralized repositories/services. Risk is cloud-based because that is where the data will reside.

- Business leaders are implementing or planning to implement a data centralization and platform consolidation strategy in response to business challenges and compliance demands.

- Performance and usability are important evaluation factors when it comes to compliance solutions procurement decision making, especially in the context of enabling remote work.

- AI and predictive analytics are taking on a growing role, providing tools to classify and handle sensitive data—including personally identifiable information (PII)—properly.
In conclusion, we recommend implementing a data consolidation and centralization strategy in conjunction with any move to the cloud. We recommend that enterprises start with data security and privacy drivers, address both tactical and strategic goals, and use the cloud as a catalyst for change. We urge companies to take an ecosystem-based approach, and to select solutions that help keep up with the changing regulatory landscape. Finally, we consider users to be a central element of success.

On this final point, the research reveals that attitudes toward remote work have changed — enterprises are ready and willing to trust staff that are working outside of the office, even as they address the risks that emerge.

### 2. What is Driving Strategy Today?

Recent months have writ large how unexpected events can arrive from nowhere and have a profound impact. Even before companies across the globe had to face challenges caused by the arrival of COVID-19, they were confronting numerous issues, both large and small, and they continue to do so even in the midst of the pandemic. From our research, conducted in the middle of lockdown, we can see the profound influence that digital transformation has on organizations, with more than 85% of surveyed companies reporting that they have either already addressed or are actively dealing with a digital transformation effort.

![Figure 1. Major Factors Driving Change in Enterprise Organizations](image-url)

**What are the Major Factors Influencing Your Organization Right Now?**

- **Digital transformation**
  - Already treated: 41.8%
  - Actively dealing with this: 45.4%
  - A future concern: 9.5%
  - Not a significant priority: 3.5%

- **Monitoring and preserving privacy**
  - Already treated: 35.4%
  - Actively dealing with this: 46.6%
  - A future concern: 11.0%
  - Not a significant priority: 6.9%

- **Keeping up with regulatory changes**
  - Already treated: 35.1%
  - Actively dealing with this: 45.1%
  - A future concern: 14.6%
  - Not a significant priority: 4.2%

- **Addressing the challenges of remote/distributed work**
  - Already treated: 31.7%
  - Actively dealing with this: 47.6%
  - A future concern: 13.7%
  - Not a significant priority: 7.0%

- **Focus on balancing efficiency and cost savings with worker productivity**
  - Already treated: 30.8%
  - Actively dealing with this: 43.0%
  - A future concern: 18.6%
  - Not a significant priority: 7.6%

- **Evolution in risk assessment approaches**
  - Already treated: 28.7%
  - Actively dealing with this: 48.5%
  - A future concern: 17.4%
  - Not a significant priority: 5.4%

- **Data growth and its impact on governance**
  - Already treated: 28.4%
  - Actively dealing with this: 52.4%
  - A future concern: 14.6%
  - Not a significant priority: 4.6%

- **Updating business strategy to address a changing landscape**
  - Already treated: 27.4%
  - Actively dealing with this: 46.6%
  - A future concern: 17.7%
  - Not a significant priority: 8.3%

*Source: GigaOm 2020*
Drilling into the data we can see how this differs by country - for example, 62% of German respondents claim their organizations have already treated it, compared to only 16% of French companies. By vertical, technology companies are ahead of the pack (58% already treated), whereas finance and manufacturing are behind (33% and 36% respectively).

So, what can we learn? From our conversations with enterprise decision makers, we know that "current times" and digital transformation are inextricably linked, as the former has forced organizations to rethink incumbent business practices and how they engage with suppliers and customers. In our survey, 74% said they were updating or already had updated their strategy to deal with the new market conditions, although only 27% listed it as a primary concern. COVID has accelerated the digital transformation timelines for many companies — we are seeing symptoms of accelerated digital transformation, as organizations stop trying to understand what it is and focus more on delivering digitally enabled services internally and externally. A significant majority (81%) were addressing or had addressed an increase in data growth, and 77% had changed or were changing their risk assessment approaches. However, in many cases, disruption from these efforts has been far less than anticipated, creating confidence to pursue further change.

As Mir Kashifuddin, Partner, Information Governance and Privacy at PwC, notes: “When the crisis hit, we saw companies struggling but also a set of leaders emerging, delivering accelerated digital journeys, omnichannel approaches and so on. What’s been most powerful is that the companies doing really well are being emulated from a business model, customer journey perspective. We’re seeing increased investment: it’s all about putting guardrails in, whether it’s privacy, data protection, insider threat or other areas, all are accelerating.”

Kevin Barnicle, Regional Vice President, Information Governance at Epiq concurs: “We initially in March saw a complete timeout - something I’ve never seen. Every single company told us ‘we don’t care about this right now.’ But then mid-April suddenly we found there was urgency around lots of projects. The shift to working from home was driving digital transformation and that raises a lot of Governance, Risk and Compliance (GRC) considerations. So now it’s accelerating. Companies that were planning on rolling out Microsoft Teams in 2021 or 2022 had to roll it out in a matter of weeks. It’s been a steady state for the last few years, now it’s a real rollercoaster.”
Digital transformation often trails privacy and compliance challenges in its wake. Says Joshua Rattan, Partner, Information Governance and Privacy, PwC, “Clients are busier than ever implementing information governance, data governance and privacy programs, despite COVID and its economic impacts — we’ve seen a significant uptick in Data Protection, Privacy, and related use cases. Clients see digital transformation accelerating the execution of information governance and privacy programs given the need to scale into the cloud, but doing so securely.”

The increasingly proactive legislation following the 2018 introduction of the General Data Protection Regulation (GDPR) already posed a challenge for enterprises. By reviewing the general feedback, we can see how the new breed of legislation pioneered by GDPR — including enforceable examples like the California Consumer Privacy Act (CCPA) — is having an effect. We found that 82% of those surveyed are working to monitor and preserve privacy, 80% are addressing or have addressed regulatory issues, and 80% are addressing issues related to data growth. All these challenges feed into the mounting issue of being compliant with new laws.

“GDPR and CCPA are driving awareness,” says Karen Schuler, Principal, Governance, Risk and Compliance Practice Leader at BDO. “More often than not companies have begun to realize the risks that data presents to an organization. Regular corporate initiatives call upon companies like us to map the locations of data and where and how it flows internally and externally. Interestingly enough, companies are always surprised by what they find. Many didn’t know what information was sent outside their organization, and they were even more surprised when they discovered it was sensitive data.”

Interestingly, the USA and Germany lead the way in tackling monitoring and preserving privacy — 42% and 40% respectively believe they have treated it, compared to 27% and 22% respectively for the UK and France. Looking ahead, the UK is the most pessimistic about its chances of dealing with the issue, with 29% reporting they expect to have dealt with the issue - only rising 2%.

Managing the risk posed by employees is still largely unaddressed.
Figure 2. Non-Regulatory Risk Sources

The survey sample (shown in 6. About the Research) was filtered on respondents with involvement or influence in GRC, so it is unsurprising that regulation is seen as important. Just as intriguing are the other sources of risk — not least from consumers themselves. High on the list are evolving consumer needs and expectations (44% consider it a primary concern, 37% secondary), and the potential for social or reputational risk (37% and 42%). The UK is the most concerned about social and reputational risk - with 48% considering it a primary concern. German companies are the least concerned with only 21% considering it a primary concern. Knowing Germany’s proactive attitude towards privacy, it is highly probable that respondents see this as less of a source of risk. Meanwhile, consumer-facing sectors such as retail and healthcare are also more concerned about social/reputational risk with customers (50% and 47% respectively).

Also interesting is the fact that challenges posed by employees using their own devices (BYOD) scored at the bottom of primary concerns with only 24% considering this a primary risk — an indication that they may have already addressed the concern. Insider threat, while identified as a primary concern by only 30% of respondents, is the number one secondary concern, reported by 48% - implying that
We can gain further insight by reviewing comments from respondents, viewed above as a word cloud. Alongside terms like Digital and GDPR, COVID, Security, Privacy, and Compliance, we can see Health and Safety, Home and Remote Working as well. On the former, respondents from the Healthcare sector were significantly more concerned about consumer needs — 63% listing it as a primary concern, compared to 44% overall. Meanwhile remote working has become the poster child for how organizations can continue to function, and even be successful, if they place trust in their staff to work away from the office, and if they direct tools, technologies, and policies accordingly. While some organizations are already welcoming staff back into offices, more flexible working practices are here to stay. This will create new and complex challenges for organizations of all sizes.

As notes Stephen Griegel, NA Data Security Lead, Accenture Security, “I hear from clients that there is a level of trust, but no way to verify it. A lot of the walls built around offices and infrastructure, from a security perspective, are no longer there, now people are working out of their homes. There’s a need to be able to know, while working from home, that individuals are handling data whilst maintaining the same security protections as in the corporate office.”

Concurs Clifford Corney, Vice President, Strategic Business Development, Cognni: “That is the
challenge: there's so many events that happen each day and because of working from home, we are forced to be secure and compliant but also working from the cloud.”

Returning to Figure 1, we see that at the bottom of the list of factors is the need to update business strategy to address the changing needs of today's landscape (27%). This is really interesting, not least because it suggests that existing strategies around digital transformation are sufficient, if they are implemented correctly. Put simply, organizations are focusing on changing how they deliver their existing services or products, not what they deliver: it’s time to stop talking about transformation and get on with the job. Data growth is also low on the list as “already treated” (28%), but note how more than half (52%) of respondent organizations are now “actively dealing with this.” The Governance, Risk and Compliance (GRC) response to data growth is essentially in a catch-up phase, a factor that we shall return to later.

3. Causes and Effects

If we turn to the most significant risk and compliance-related challenges, we can see how the fast-evolving regulatory landscape stands out as a primary challenge across our respondent base (45% of organizations). Schuler says there just are not enough resources to go around.

“There’s been an onslaught of additional guidance recently, as well as regulators commenting on COVID and how personal data related to contact tracing or wellness apps should be handled, and we’ve found that companies are not adequately prepared to fully train personnel and do not have enough personnel to satisfy their regulatory obligations,” Schuler says.
Figure 3. Risk and Compliance Challenges

It is interesting to compare these results against the next three challenges:

- Having day-to-day visibility on measures and goals — 87% cite it as a primary or secondary challenge
- Managing a fragmented solutions base — 80% have as primary or secondary
- A lack of clarity around roles and responsibilities — 71% as primary or secondary

Essentially, if the main problem is keeping up with regulation, then deployed tools and approaches do not help — organizations are pushed onto the back foot through no fault of their own. Note from the chart that other, more internal issues (such as organizational silos or inconsistent use of compliance frameworks) may exacerbate, but not cause, this situation.
Drilling into use of information and data, we see how the continued, rapid growth of unstructured data — that is, documents and media files — stands out as a factor above all others, with 87.2% of organizations seeing it as a significant challenge. Data growth interplays with the dynamism of the regulatory landscape, creating a perfect storm for decision makers. Behind data growth emerge issues of information sharing — 38% see as a main concern — followed closely by challenges posed by data fragmentation and quality, which 37% see as a primary challenge. This latter challenge can result in fragmentation of customer data, which directly affects visibility and makes digital transformation harder. Note that data quality affects health care very significantly, according to the survey respondents, with 50% considering it a primary challenge.

![Turning Specifically to Information and Data, What Would You See as the Main Challenges?](image)

**Figure 4. Information and Data Challenges**

If we look at the data protection challenges organizations are looking to address, we can see how external threats are front of mind — specifically, direct hacking of systems and services and cloud-based data breaches. More than half those surveyed, 52%, see it as a primary concern. “It’s a common misconception that people could send data to the cloud and it would be secure by design, but allowing someone to log into a cloud-based solution from an unmanaged asset is a big security risk. The response, for example setting configuration and controls, is all on whoever is setting up and managing the cloud,” says Griegel.
This cloud point builds on the issue we have seen already, that insiders are not seen as a primary threat the way external threats are. Still, internal threats remain a challenge: “Internal theft is still a big problem - mostly related to salespeople leaving an organization to join a competitor with an existing customer list. It’s so hard to protect against that because you can’t stop people printing, or taking pictures, even if you prevent files from being downloaded,” says Schuler.

![Diagram: What Data Protection Challenges Are You Looking to Address Right Now?](image)

Figure 5. Current Data Protection Challenges

It is worth digging into the second-ranked item in the chart in Figure 5, which concerns breaches of data stored in the cloud — with half seeing it as a primary concern (50%). In the very next chart (Figure 6) focused on security-related risk, we see that the cloud here is considered a primary driver of security risk (48%), above other new technologies (38%), or the pace of technology change (36%). Interestingly, technology, hardware, and software firms perceive a higher risk in cloud-based models - 61% of companies in this sector consider it a primary challenge. Healthcare, conversely, reports a much lower perception of risk (70%).
Why might this be? In part, we can see the “cloud challenge” as a straightforward consequence of the ongoing journey many organizations are making to the cloud — if data is in the cloud, then so is a risk.

The journey is one way only. Considering unstructured data, for example, five years ago we might have expected to see the majority of documents stored in on-premises file shares, yet today we see nearly two-thirds (66%) of organizations using cloud-based document storage. This creates challenges of its own, says Corney: “There's been a major change in what traditionally you would keep on your hard drive. And we see that a lot of our clients instruct their employees to move information from their hard drive storage into cloud storage for business. They want to be in control but don't know what employees are sharing.”
Figure 7. Current Work Environment

Note that this trend toward the cloud is not exclusive of other choices: over half of respondents are still using on-premises file shares today. In two years’ time, we can expect the gap to widen, with the use of cloud-based documents expected to increase to 74%, and in-house to drop to 45%.

The US and UK are more heavily invested in cloud-based repositories for sharing (with 72% and 73% respectively), compared to Germany and France (55% and 50% respectively — though these figures are expected to increase to 64% and 67% respectively in two years). By vertical, only 50% of healthcare respondents and 56% of finance respondents are using cloud-based repositories for document sharing today, but these expect to move to 80% and 70% respectively in two years.

We will pick up on this trend toward cloud-based repositories later when we talk about data centralization.
We should note that the cloud is not inherently less risky than on-premises for data storage, however the risks are different, depending on data types and usage models. Wherever it is stored, unstructured data needs to be treated with particular focus on both security and compliance. Schuler explains: “Unstructured data is where we find people sending PII to unauthorized locations. We typically find that security is better around structured rather than unstructured data... Ransomware and phishing is where most risk is coming from today.”

There is good news around unstructured data. Organizations are already looking to migrate to the cloud, and this creates an opportunity to both consolidate data and benefit from cloud-based capabilities. At the same time, cloud-based management capabilities are able to address many of the issues organizations face today. Says Rattan “The complement of information governance and privacy features that cloud solutions are providing today, is making this more of a solvable problem. For example, using labeling, IP classifiers, etc, there’s more capability in terms of understanding what data you have and governing it. The move to cloud becomes an incentive, given the features now available.”
4. What To Do In Response?

So far in this report, we have seen how external factors such as regulatory complexity, consumer pressure, data growth, a distributed workforce, and a locked-down business landscape all put pressure on enterprise GRC — and all this is added on top of the demands created by remote work. At the same time, weaknesses in existing tooling and data infrastructure make it hard to respond. So, what are organizations doing to address this challenge? From respondents we can see how a strategy of integrating and consolidating data is of highest priority: if complexity is the problem, simplification and tooling reduction is seen as a fundamental part of the solution — 54% of respondents have it as a primary concern. Consolidating data into fewer centralized, secure repositories can help create more visibility and, ultimately, more control.

![Figure 9. Mechanisms and Strategies for Responding to Enterprise GRC Challenges](image)

Barnicle concurs: “If you know what the document is, you can do lots of things: you can manage it. You know how to store it, where to store it, and how to give the right people access to it and if you need to, you can find it easily. You can also properly secure it and it makes analysis straightforward. If you know a certain set of files have social security numbers in them, you can secure them and control who can access and change them.”

From a country perspective, Germany stands out in attitudes toward integrating and consolidating data. The US, UK, and France all consider it a primary response to their data challenges (59%, 61%, and
57%) whereas Germany shows much less concern (30%).

It is interesting meanwhile, how dashboards sit at the bottom of the chart in Figure 9, with only 33% considering them a primary concern — while a lack of visibility may be a symptom of the problem, simply adding dashboards won’t fix it without having a consolidated, coherent view across data assets. Meanwhile, consolidation enables the second item in this chart, specifically automation (with 84% of respondents considering it a primary or secondary response). It also helps drive simplification of the platform, thinks Griegel. “You’ve got tools that do discovery, control, and so on, it’s a fragmented ecosystem so the consolidation of the platform that’s securing and managing data is a good thing.”

Consolidation enables the centralized definition and management of data governance policies, which can then be applied coherently to do things like automate document distribution or restrict access — understandably, it is important to address consolidation in the right order. “There needs to be a focus on centralization of management, and understanding of the data, as that’s going to be a pre-requisite before any consolidation of the data can take place. You need to understand how data is being used “in the wild,” before you can focus on data consolidation.” This point is emphasized in the chart below.

![Figure 10. Compliance Capabilities](image)

Together with consolidation, the role of centralized management is a clear priority, particularly with unstructured data, as 87.5% of organizations are considering a response of some kind. “Unstructured data is a major source of risk. With structured data, we can tackle it in a controlled manner but with unstructured, it’s a large source of potential risk, in the form of intellectual property or customer
information, which is difficult to control,” says Kashifuddin. PwC colleague Rattan explains the motivation for change: “Properly governing data - especially unstructured data - is increasingly highlighted through data breaches or a discovery request. As more examples come out that show how unstructured data is an exposed problem, these examples create increasing incentives for organizations to deal with it.”

Indeed, even if it isn't possible to move all data into one place, the ability to manage it in a unified fashion is vitally important (we see this particularly in Germany, where 57% of German companies consider it a primary response). APIs that are comprehensive and aid integration can support this centralized management model, keeping governance and protection issues to a minimum.

This brings us to the fundamental criteria upon which any such mechanisms should be judged. When we asked what was driving decision making, top of mind was performance - 57% listed it as a primary concern — followed by ease of use (46%). In other words, a mechanism will only be adopted if it works well for end users. You could go so far as to say that a security solution may be judged to be only as good as its UX — a secure yet unusable infrastructure is simply not viable.

Anecdotally, we have been told that a difficult-to-use system in a remote work setting results in employees creating workarounds, such as emailing links to themselves or sharing logins, which can put the organization in more peril both on a security and compliance footing. Interoperability across the tools an organization is using is also a critical element of successful solutions, especially in a hybrid environment. This is a very important element for companies with less than 10,000 seats — 52% list as a primary criterion in risk decision making, as opposed to 35% for larger companies. Perhaps larger companies are less likely to have employed point solutions and bought large-scale, integrated solutions.

The lesson is clear: Performance and features must be combined with smooth and easy interfaces that fit with user needs.
In terms of response, decision-makers may be swayed in favor of using AI/ML to deal with compliance challenges. Yes, these capabilities are seen as useful, notably around consumer privacy, and most especially with regard to personally identifiable information (PII) that can be buried within emails and other documents: 49% place it as a primary response.
Figure 12. Use of AI/ML/Predictive Analytics in Compliance

Such tactical use is seen as important because of the ability to monitor for and pre-empt threats, which is likely to become increasingly prevalent, explains Corney:

“Human beings cannot handle the amount of information generated by the events that happen every day. If you look at a company that has 1,000 employees, for every employee there will be between 10 to 20 events per day — just sending a file via Teams or a OneDrive download could trigger an event. Now you have 10,000 to 20,000 events happening per day. This is why AI is becoming so common in GRC. It is needed not only to monitor the events, but also to understand the context and know when activity should be flagged, and when it shouldn’t, to ensure the smooth operation of the enterprise.”

As a final point, those working in the compliance and governance sphere will know that people and processes are as important as tools when it comes to a solution. When we asked about specific actions being considered to drive strategy forward, first on the list was to increase the roles and responsibilities of the GRC function (63%), and a close second was to share decision making between business and IT roles (61%). Note that Increasing the responsibility of the GRC function is seen as even more vital in the UK and US (73% and 68% respectively).

In other words, GRC needs to be considered both more strategically, and more broadly and collaboratively. It is time for GRC to come out from its back-room position and take a front-foot position,
involving technical and non-technical stakeholders across the organization.

Figure 13. Actions Taken to Implement

5. Discussion and Conclusion

We can see how much compliance criteria are affecting organizations today and how they will continue to do so. These pressures are pushing decision makers onto the back foot as they look to deal with a changing set of priorities while lacking the tools and visibility they need. We have seen how a centralization strategy can help, both in specific terms (by consolidating data into a fewer cloud repositories) and more broadly through adoption of centralized management and automation of policy.

Based on the research in this report, we believe a strategy of centralization is the key starting point for any organization looking to take control of its data and optimize its use across systems, territories, and business units. To deliver on this goal, we recommend taking the following points into account:
Start With Data and Privacy Drivers

With a distributed workforce and distributed data, it becomes “business critical” to understand your data — where it is, how it is being used, and who it is being shared with. Starting with these drivers also means starting collaboratively, to understand general needs and challenges. This fits with the second priority shown in Figure 13.

This enables organizations to gain more of a view of what they have — which is a pre-requisite of success, says Corney: “So many of our clients have security tools, but the implementation takes a very long time because they don’t know how to map the information they have. Where is my financial information? Where is my HR Information? Where are my board documents’ legal information? This information is now being moved to the cloud, because the cloud is easier to manage, but they still lack visibility. It’s easier to be in control, but you still need to map that information and understand where it is. Then you can actually take the right action.”

“Understanding your data is a clear business need, but with recent regulations it is an absolute must-have. I’ve never seen so many requests for data identification, data flow mapping, retention and data classification as I have over the last year — it’s the new normal.” says Schuler, Governance, Risk and Compliance at BDO.

Address Both Tactical and Strategic Goals

While it is tempting to target lower-hanging fruit, decision makers should also be thinking about longer-term goals and priorities that will affect the broader business. You can work on a department-by-department basis to reduce dependencies, bringing relevant stakeholders together to collaborate on policy setting and have them act as internal champions in their own areas. As per Figure 13, this also creates an opportunity to give the GRC function a broader, more facilitative role.

Barnicle said: “Many companies are in analysis paralysis, and are trying to boil the ocean. We advise them to just get started, and often propose working with just one department to start to understand the process. Often companies have done nothing for five years and they have called us because they are dealing with the fallout from failing to act.”

Given the complexity and dynamism of data, centralization cannot be seen as a one-shot operation (however big). Rather, it should be viewed as a program that delivers value over time. The advantages of this approach are that it can demonstrate and deliver value earlier, freeing resources and developing goodwill. Therefore, label the project as a change program with a clear name, mission, and objectives.
Use the Cloud as a Catalyst For Change

We have noted how the ongoing move to the cloud offers an opportunity to centralize unstructured data assets and benefit from the consequences of having data in place through its lifecycle and sharing. It makes sense that centralization is based on where the majority of documents will be. We realize, of course, that this effort will not always be straightforward, but having a clear target (such as a consolidated cloud-based repository) will help with efforts to get on top of data sources and flows. “We need to be able to find where it is, there’s no silver bullet solution. We follow the data, then understand whether data is flowing from on-prem, to cloud, to third-parties,” says Kashifuddin.

One such repository is Microsoft 365, explains Barnicle: “Many companies we work with have a huge amount of legacy data and applications, such as email systems and document management systems that they don’t need anymore. We advise them that they are already paying for a very powerful tool that can take care of this data and these services: it’s called Microsoft 365. So we help them migrate their data to the cloud, and that lets them gain visibility and control of their data, whilst making cost savings on these legacy systems they were paying for.”

Take an Ecosystem-Based Approach Driven by Visibility

Data stores, GRC systems, and cloud-based services need to be integrated with legacy systems (often still needed on-premises) and hybrid storage solutions to create a package that caters to the needs of the entire organization, supporting the principle of "security by design" shown in Figure 13. The key to utilization is the compatibility of platforms and their ability to integrate smoothly with data and GRC solutions, for example, via comprehensive APIs and connectors.

“I’m a big proponent of getting visibility into the data estate - this visibility helps inform control frameworks, define control requirements, and how to identify near-term wins. Governance is also key, understanding information governance program ownership being critical - information governance is such a multi-faceted issue requiring cross-department collaboration including legal, privacy, compliance, information security, etc. So you need to ask where does the ownership and accountability lie, so you can drive information governance efforts forward and deliver real results.” says Rattan, Information Governance and Privacy at PwC.

Consider Users as a Central Element of Success

We have seen the importance of performance and usability for any solution, but this is only one part of the story. For example, in the course of consolidation, you can consider the possibility of incentivization, promoting the benefits of making such a move (such as guaranteed availability, relative to local copies of files).
“Tools need to be easy to use, they can’t be confusing or convoluted. For example, with classification, a whole lot of education and re-education has to go into that to make it less confusing. How do I share a document externally, in the right way, can be extremely difficult. Which means keep it simple!” says Griegel, NA Data Security Lead at Accenture Security.

From a policy-based perspective, you can define must-have versus nice-to-have policies and communicate these clearly to staff, in such a way that balances the dual needs for security and compliance, with user productivity and wellbeing. Note that heavy-handed implementations will motivate business users to look for workarounds that will increase the chances of a data breach.

Overall, the challenge may be external, but the response is all internal. It is worth re-emphasizing the wave of increased employee trust we have seen around remote working, which is something to be built upon. Even if the main challenges are dynamism, complexity, and fragmentation, all solutions need to allow business users to get on with their daily jobs.

6. About the Research

The study involved 328 interviews with strategic IT decision-makers in enterprise organizations across North America and Europe. The research took place over June-July 2020. It was sponsored by Microsoft.

![Figure 14. Audience Geography](image-url)
Respondents were filtered according to company size, and whether they had direct involvement with or influence on strategy and technology procurement decisions, specifically relating to risk and compliance.

Source: GigaOM 2020

**Figure 16. Audience Organizational Roles**
7. Acknowledgements

GigaOm would like to thank Accenture, BDO, PwC, Epiq, and Cognni for their participation in the research.

8. About Microsoft

Microsoft (Nasdaq “MSFT” @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

- Hemma Prafullchandra, CTO of Microsoft 365 Security and Compliance
- Kacey Lemieux, Director of Product Marketing at Microsoft, Information Protection, Governance, Privacy
- Hammad Rajjoub, Director of Product Marketing at Microsoft, M365 Compliance Ecosystem

9. About Jon Collins

Jon Collins has advised the world’s largest technology companies in product and go to market strategy, acted as an agile software consultant to a variety of Enterprise organizations, advised government departments on IT security and network management, led the development of a mobile healthcare app and successfully managed a rapidly expanding Enterprise IT environment. Jon is frequently called upon to offer direct and practical advice to support IT and digital transformation strategy has served on the editorial board for the BearingPoint Institute thought leadership program and is currently a columnist for IDG Connect.

Jon wrote the British Computer Society’s handbook for security architects and co-authored The Technology Garden, a book offering CIOs clear advice on the six principles of sustainable IT delivery. He has written innumerable papers and guides about getting the most out of technology and is an accomplished speaker, facilitator, and presenter.
10. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm’s advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm’s perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

11. Copyright

© Knowingly, Inc. 2020 "Digital Risk, Compliance, and Data Centricity" is a trademark of Knowingly, Inc.. For permission to reproduce this report, please contact sales@gigaom.com.