CREATING A FRAMEWORK FOR SUCCESS IN THE CLOUD WITH CLOUD GOVERNANCE

Authors:
Carla Arend
Ralf Helkenberg
Denis Maslennikov

March 2021

Sponsored by Microsoft

IDC Partner Spotlight
Creating a Framework for Success in the Cloud with Cloud Governance

Introduction

AT A GLANCE

CLOUD TRENDS

• 84% of European organizations operate hybrid and multicloud architectures.
• Cloud is an operating model and an architecture, not a location.

CLOUD GOVERNANCE

Cloud governance is the glue that binds cloud and data strategy together and provides a framework for success in the cloud.

BENEFITS OF CLOUD GOVERNANCE

• Unlock business value
• Optimize cloud cost and utilization
• Increase operational efficiency
• Reduce compliance and security risk
• Improve data productivity

As cloud becomes mainstream it can unlock significant business value. Time to business value can be accelerated if cloud is viewed as an architecture and an operating model, and not as a location. Hybrid and multicloud architectures are becoming the most common operating model, with 84% of European organizations operating a combination of on-premises IT and public cloud. The benefits of cloud as an operating model and an architecture were proven in 2020, and European organizations are modernizing their on-premises IT estates towards a cloud architecture, and migrating workloads into the public cloud for greater agility and flexibility and to improve their response to change.

IDC believes that:

*Through 2023, European enterprises will focus on application modernization and data integration across cloud silos; 20% of European organizations will adopt connected cloud architectures to overcome these concerns.*

To create a cloud-based IT architecture that enables the business to respond quickly and adequately to changes in the market, and to manage IT infrastructure efficiently across on-premises and cloud-
based IT, applications, and data, European organizations are restructuring their cloud and IT management approach. They are embracing policy-driven, automated "connected cloud" architectures that abstract away underlying cloud-specific dependencies via the deployment of standardized, cross-cloud governance and control APIs designed for flexible, dynamic, connected cloud operation.

Governance across connected clouds is the glue that holds cloud strategy and data strategy together and provides a framework for success. Hybrid and multicloud architectures can provide complex integration challenges with the security and regulatory environment and need for compliance. The latest cloud governance tools and processes simplify the overall cloud journey, but also help to identify and mitigate security and compliance risks that had not been addressed in legacy environments, while also unlocking value from cloud-based innovation.

What is Cloud Governance and Why is it Important?

Cloud governance is a set of rules and controls that is intended to enable IT modernization, cloud migration, and business innovation while identifying and mitigating security and compliance risks. The first step to cloud governance success is to identify potential issues through an effective assessment, before the mitigation can take place. Organizations need to implement cloud governance to address the following issues that can arise along their cloud journey:

Operational Complexity and Cloud Cost Control

Operating a hybrid and multicloud infrastructure provides the benefits of agility and innovation but poses the challenge of operational complexity and cloud cost control because every IT environment is managed differently. Driving one policy across the entire IT estate through cloud governance increases efficiency, observability, and cost control.

Data Sprawl and Siloed Data

One of the key challenges that emerges when spreading IT infrastructure across on-premises and cloud locations is the sprawl of data and the creation of new data silos across the cloud. This not only creates operational complexity but also creates challenges in terms of cost and risk management. Cloud governance tools and practices help to keep track of data regardless of location.

Regulatory Compliance and Security

Security and compliance continue to be the biggest concerns when European organizations are planning their cloud journey. To ensure successful cloud modernization, cloud governance needs to be put in place early in the cloud modernization process and improved over time to align with evolving business requirements and regulations.
Regulatory frameworks supporting or complementing privacy and data security legislation are developing rapidly. Understanding regulatory requirements and operationalizing a governance structure that is responsive to regulatory developments is a growing challenge, and an inhibitor to technology adoption, particularly where organizations lack resources and expertise. Though organizations are moving their computing infrastructure to the public cloud, the most important inhibitors to faster adoption are privacy and security concerns. IDC's 2020 multicloud survey showed security and compliance with data protection ranked as the most challenging to execute in a hybrid, multicloud environment.

**FIGURE 1**
Adoption of Cloud Services

Survey question: Which data services are the most challenging to execute in hybrid and multicloud environments?

- Security and compliance: 44%
- Data protection: 43%
- Integration and orchestration: 35%
- Data location optimization: 33%
- Data migration and repatriation: 30%

Source: IDC's 2020 annual multicloud and next-generation infrastructure survey N=1,187

**Data Governance**

Ensuring the availability, integrity, usage, and security of data takes on an additional dimension of complexity in hybrid multicloud environments. Complete data visibility is foundational to any effective data governance program, yet is a blind spot for many organizations. Data proliferation has created data silos where organizations have little insight into what data is available, where it comes from, how it is used, and whether it is trustworthy. Data tends to be in everybody’s interest but often is nobody’s responsibility: privacy, security, and data governance can benefit from having one source of data truth, thereby ensuring consistent and compatible business decisions.
Cloud Governance Trends and Challenges

Cloud adoption is on the rise because using cloud platforms is an opportunity for business and organizational units that were previously operating independently to work together. Cloud provides a significant opportunity to streamline processes for faster innovation, but the complexity of bringing different operating units together should not be underestimated as it is often the cause of delay in cloud projects. Business alignment across the organization can be accelerated by adopting a consistent cloud operating framework.

Hybrid and multicloud architectures are moving to the mainstream, with 84% of European organizations operating on-premises IT assets as well as multiple public cloud services as part of their IT landscape. 16% of European organizations have a cloud-first or cloud-only strategy, while 14% are still operating entirely on-premises, according to IDC's annual multicloud survey.

FIGURE 2
Attitudes to Cloud Adoption

We are only just starting on the cloud journey — the destination is hybrid cloud

While on average 84% of European organizations are operating a mix of on-premises IT and cloud services, there are significant country-level differences in terms of attitudes towards cloud adoption. According to IDC's 2020 annual multicloud and next-generation infrastructure survey, between 70% and 89% of organizations are operating a mixed-hybrid IT infrastructure, with Italy at the top of the list and Austria being more conservative in their approach to cloud (see Table 1). Despite these differences, the trend is clear: the future of IT is hybrid, and organizations need to address operational and governance challenges to be successful in this hybrid IT world.

Source: IDC’s Annual Multicloud and Next-Generation Infrastructure survey, N=1187
TABLE 1
Percentage of Organizations Using Hybrid IT by European Nation Plus Biggest Cloud Challenge

<table>
<thead>
<tr>
<th>European Country</th>
<th>% of organizations using hybrid IT</th>
<th>Biggest cloud challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>89%</td>
<td>Data sovereignty concerns</td>
</tr>
<tr>
<td>Switzerland</td>
<td>88%</td>
<td>Security</td>
</tr>
<tr>
<td>Spain</td>
<td>87%</td>
<td>Security</td>
</tr>
<tr>
<td>Germany</td>
<td>85%</td>
<td>Skills shortage</td>
</tr>
<tr>
<td>Portugal</td>
<td>85%</td>
<td>Trust</td>
</tr>
<tr>
<td>Nordics (Denmark, Finland, Norway, Sweden)</td>
<td>84%</td>
<td>Reliability</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>84%</strong></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>83%</td>
<td>Cost</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>82%</td>
<td>Skills shortage</td>
</tr>
<tr>
<td>Poland</td>
<td>81%</td>
<td>Software licensing</td>
</tr>
<tr>
<td>France</td>
<td>79%</td>
<td>Security</td>
</tr>
<tr>
<td>UK</td>
<td>79%</td>
<td>Security</td>
</tr>
<tr>
<td>Austria</td>
<td>70%</td>
<td>Data sovereignty concerns</td>
</tr>
</tbody>
</table>

Source: IDC Annual Multicloud and Next-Generation Infrastructure Survey, 2020

The challenges when adopting cloud vary country by country and range from data sovereignty concerns, security, and trust issues to skills shortage, reliability, and software licensing issues. As organizations progress on their cloud journey, they are looking for solutions that address these challenges.

2020 has brought a major shift in mindsets in Europe, where organizations have moved from "if" they should use cloud services to "how" they can best operate a hybrid multicloud architecture.

Key challenges that they have encountered in their cloud modernization revolve around security, compliance and trust, performance issues and a very pronounced skills shortage. To enhance the success rate of cloud modernization, these areas need to be addressed, and cloud governance is a structured approach to do so. **Cloud governance is an emerging area, highly effective if done right, but currently not very well understood by most organizations.**

**The Benefits of Cloud Governance**

A cloud governance model delivers the blueprint for building and operating your cloud environment or services. The key benefits of a cloud governance model include:

**Unlocking business value:** A governance framework ensures cloud usage is aligned with business objectives and offers businesses the trust and confidence to advance new cloud-based business
models and outcomes, with better productivity, lower costs, faster digital innovation, and smarter insights, while ensuring business continuity, resilience, and security are preserved. However, the complexity of bringing siloed parts of a business to work together across the cloud should not be underestimated. A consistent cloud operating framework can be the glue to ensure operational alignment between business areas.

**Optimizing cloud cost and utilization:** Commercial and technical teams often do not have the right oversight and capability to properly optimize cloud costs. Cloud optimization aligns cloud resources with business needs more promise of realizing reduced TCO. Policy based cost governance for current and future cloud operations ensures cloud service usage is predictable, reasonable, and accountable.

**Creating operational efficiency:** Architecting for hybrid cloud, particularly where multiple providers are involved, is not an easy undertaking when it comes to workload management, orchestration, and integration. A cloud governance framework provides a centralized, consistent, and agile deployment and resource management model, thereby avoiding operational pitfalls that increase complexity, cost, and risk. Alerts can be set up to notify organizations whenever escalations or deviations happen from the defined desired state. Faster deployment and configuration of new and updated services in the cloud is also achieved through centralization, consistency, and standardization of deployment templates.

Belgian IT managed services company DexMach helps European organizations with their cloud modernization. Optimal infrastructure configuration and management in hybrid environments is often constrained through partial or siloed infrastructure visibility and the inability to integrate on-premises policies and updates with cloud-based operations. By leveraging Microsoft Azure Arc, DexMach can manage infrastructure, policies, and services for these clients across their entire hybrid estate, all from a single platform.

**Reducing compliance risk:** regulatory compliance is influential in shaping the business approach to data privacy and protection in the cloud. Cloud governance helps to maintain compliance by monitoring cloud configurations against regulatory requirements, addressing open violations, and enforcing rules and audits. Compliance as code offers a fast and effective way to validate regulatory compliance. Automated test script deployments eliminate manual audit bottlenecks and enable real-time feedback and resolution to compliance deviations.

**Mitigating security risk:** Operating across on-premises, edge, and multicloud broadens the attack surface. The higher security exposure necessitates businesses to extend their on-premises security and governance policies to cloud infrastructure and services. Cloud governance provides the platform to audit and monitor the observance of security policies and controls, identify gaps, and mitigate them before they become threats.
Improve data productivity: A lack of visibility into growing volumes of data across hybrid cloud infrastructure leaves organizations at a privacy compliance and business disadvantage. Automated sensitive data discovery with a centralized cloud governance approach ensures data policies are consistent throughout the IT infrastructure, including the granting of data access requests.

Cloud Governance Best Practices

Enterprises often embark on cloud initiatives without being properly prepared for the complexities they will encounter. Only once the cloud footprint becomes substantial enough and concerns around security, cost, scale, and operations arise does cloud governance become a serious consideration.

Cloud governance and enablement is an organizational discipline, not a technology. It requires a vision, people, process, policy, and technology. Designing and implementing a best-in-class cloud governance framework takes time and effort. Too often technology is sought in hindsight as the answer to cloud governance and enablement problems, but it is only part of the solution.

Business Alignment

There is no one-size-fits-all approach as each organization will have its own unique set of processes and needs that must be considered when developing an effective governance strategy and management plan. These plans should determine the direction and objectives of cloud computing and exploit the opportunity to fully align IT with the strategic goals of the enterprise and add value to the organization. By using a Cloud Adoption Framework, organizations can better align and shape their business and technical strategies with desired business outcomes during their cloud adoption efforts.

Governance Accountability

A lack of structured decision making around cloud service provision is a common cause of lack of governance direction. A Cloud Center of Excellence can provide the leadership structure to ensure the governance strategy, framework, policies, and best practices are appropriately formulated and implemented. Broad representation from corporate, departmental, and IT management helps to strengthen communication and advocacy for the strategy across the organization.

Risk Tolerance

Organizations should determine their level of risk tolerance and adopt a risk-based approach to properly categorize and evaluate perceived risks in terms of both potential negative impact and positive opportunity. Using a Cloud Adoption Governance Framework will help guide this process, including areas of shared responsibility. This includes risks that are managed exclusively by the organization, where there is shared management of risk with a cloud provider, and where the cloud provider manages the risk exclusively. This will help to identify key business areas of importance and associated risks and guide required actions and policies.
Iterative Governance

Cloud modernization is a "journey, not a destination." As the cloud infrastructure evolves through changing business requirements, so must cloud governance move quickly and keep pace to stay relevant. Adopting an incremental model approach to governance is recommended. As a foundation, build a minimum viable product (MVP) — a small set of corporate policies, processes, and tools that align with the business goals and strategy. Once deployed, additional layers of governance can be incorporated as cloud maturity and footprint grows.

Digital and Data Visibility

For systems and applications to work effectively in a hybrid environment, organizations need to know what policies they want to enforce on what data workloads and when. You cannot optimize, control, or secure what you cannot see. Best practices for data governance in the cloud are data discovery to determine what data assets there are and sensitive data classification to inform which governance policies and procedures apply to the data. Similarly, when defining a hybrid cloud strategy, it is important to understand the profiles of the workloads that will run in the cloud — what the applications do, from how they interact with users, manage data, and handle networking to their performance and security profiles.

Cloud-Enabled Workforce

Digitally transforming with the cloud requires more than just IT. Cloud governance must not only address the modernization of the cloud infrastructure, but also what skills and capabilities are needed to cloud-enable an organization's workforce. This includes familiarity with the concepts and execution of cloud governance and best practice. Bridging the cloud skill gaps requires delivering a talent outreach and enablement program through a combination of hiring, outsourcing, knowledge sharing-tools, and training.

Vendor Profile

Cloud has become the foundation that enables businesses to transform, innovate, and gain competitive advantage. The hybrid-cloud approach, though favored by many organizations, creates operational, security, and compliance challenges. Recognizing the diversity in IT environments and appetites to moving sensitive workloads to the cloud, Microsoft's cloud product strategy is geared toward delivering solutions that address the many architectural and operational complexities that IT teams face with today's hybrid cloud scenarios.

Microsoft Azure Arc

A central pillar of Microsoft's hybrid cloud strategy is Azure Arc, a management control solution that enables organizations to manage their entire hybrid infrastructure through a single pane of glass. The platform extends visibility and control of Azure Resource Manager to on-premises, edge, and cloud deployments, and allows for remote operation of Azure infrastructure and data services.
instances using the same tools and templates as the Azure public cloud environment. This centralized control plane permits organizations with legacy infrastructure to embrace a "run anywhere" approach and to deploy Azure data services, Kubernetes applications, and virtual machines quickly and consistently across chosen environments and without compromise in cost, governance, and performance. Where regulatory and data sovereignty concerns are high, IT teams use the same configuration management to ensure consistent policy enforcement to meet compliance, privacy, and security requirements.

**Microsoft Azure Purview**

A unified data governance platform, Azure Purview is part of Microsoft's vision for a unified end-to-end platform for data management and analytics. Just like people use search engines to find content on the internet, a data discovery engine searches for data across the hybrid enterprise estate to inform compliance and governance strategies and drive smarter data intelligence and decision making. The data catalogue is populated with scanners that crawl across the on-premises and multicloud data estate and classifiers that identify data type, location, and sensitivity level and relationship to other data assets. The classifiers included can support compliance with privacy laws such as GDPR as well as industry-specific regulations. The catalogue provides the platform for creating a unified graph-based map of data assets across hybrid cloud environments. Data lineage capabilities are enhanced through Microsoft environment integrations with Power BI, Data Factory, Synapse Analytics, SQL Server, and Microsoft 365. Apache Atlas APIs offer further flexibility to incorporate third-party and partner data environments.

**Microsoft Cloud Skilling**

A lack of internal skills and knowledge is a top barrier to cloud success. Microsoft recognizes that technology alone will not enable organizations to realize the benefits of the cloud and offers customers a full suite of learning opportunities to build and strengthen their cloud capabilities. The options are flexibly tailored to customer needs, from cloud role-based training to specialty training courses that cater to specific cloud projects or applications. Learning is enhanced with hands-on experience with Azure Labs, delivered in easy-to-access, free sandbox environments.

**Challenges**

Hybrid cloud architectures are operationally complex for customers, and customers are challenged to converge their cloud strategy and data strategy to meet compliance and operational requirements. These topics are often dealt with by different teams within European organizations. Microsoft will need to join its product development, marketing initiatives, and partnership strategies to create a holistic methodology for its customers. Partners play a key role in creating a holistic strategy, as they help customers to build data management programs, classify their data, and identify and manage risk.
Security is still the biggest obstacle to successful cloud adoption. Although Microsoft shows up as the most trusted cloud provider in IDC surveys, the company needs to continue to educate the market about best practices in cloud modernization, operation, and security.

There is skepticism in Europe toward US-headquartered cloud providers due to the CLOUD Act\(^1\). Microsoft Sweden is using a mixture of training and advisory support on how to run sensitive workloads in the cloud in a compliant manner. This initiative could function as a template across Europe.

**Conclusion**

IDC expects cloud architectures spanning private cloud datacenters, edge, and multiple public clouds to be the enterprise norm due to concerns around cost, security, data privacy, and compliance. While the lift and shift approach to cloud modernization may appear to be an efficient way to go, it typically does not deliver the full advantages of the cloud in the longer term. Too often there is a reliance on disconnected and divergent infrastructure management, governance, and monitoring mechanisms, which are hard to maintain and automate at scale. The result is that agile cloud-based deployments often collide with traditional deployment, operations, and security strategies — creating significant business friction.

IDC believes cloud governance is foundational to building and managing a successful hybrid cloud infrastructure. The three crucial aspects of successful governance are people, processes, and technology. The Microsoft Cloud Adoption Framework for Azure provides businesses with an operating model to enable organizational and technology change management and, irrespective of the chosen cloud approach, inform decision making with a well-proven library of best practices, documentation, and tools. A range of Microsoft learning and certification opportunities allows organizations to upskill their workforce with the right skillsets and knowledge to drive digital transformation.

Microsoft has been at the forefront in delivering solutions that emphasize public cloud-centric deployment models deployed on premises. Given the much-cited governance and security challenge, Azure Purview provides a timely solution to organizations seeking data visibility. The automated data discovery and classification works across on-premises, multicloud, and SaaS environments, making the task of creating holistic up-to-date maps of the data landscape significantly easier and quicker. Cloud governance best practice demands ongoing due diligence and oversight across environments. Here Azure Arc offers customers the operational flexibility to deploy and scale Azure data services anywhere, yet also have assured control over resource configuration, compliance, and security.

---

Glossary:

- **TCO**: Total cost of ownership (TCO) is used to compare the true cost of different IT solutions (on-premises and in the cloud), including investment in IT hardware and software, services, personnel, facilities, and energy consumption. It is used to compare the total cost of a cloud service with the total cost of an on-premises solution.
- **Cloud Center of Excellence**: Organizational group that develops best practice guidelines for cloud usage for the organization. The CCoE drives the organizational transformation that is necessary to take full advantage of the benefits that cloud can deliver.
- **Public Cloud**: Shared IT infrastructure operated by a public cloud provider that can be accessed through a self-service portal.
- **Hybrid Cloud**: Connection of on-premises IT with one or more public cloud services, may also include Edge computing solutions, that is integrated and may have a single management layer.
- **MultiCloud**: Usage of multiple cloud services managed with a single management layer.
- **Compliance-as-Code**: Automates the implementation, verification, remediation monitoring, and reporting on compliance rules and status of compliance in the management software layer.
Navigating a hybrid cloud strategy while effectively managing risk is top of mind for our customers. A hybrid strategy enables faster innovation and provides flexibility for multicloud deployment, on-premises, remote locations, outsourced hosters, or at the edge. A consistent cloud operating model is required to control and govern these increasingly complex environments. This provides a foundation for risk management for data, compliance, security, and privacy.

Microsoft has unique offerings including Azure Arc, Azure Purview and the Azure Stack portfolio to support a hybrid strategy, while enabling transparency for informed decision making.

Azure Arc simplifies governance and management with a consistent multicloud and on-premises management platform, including features that translate requirements into "compliance-as-code". Azure Purview for Unified Data Governance enables automated data discovery and classification no matter where the data resides, creating a unified map of data assets for more effective governance. Azure Stack extends Azure services to the datacenter and the edge, providing flexible deployment options to meet regulatory requirements.

Learn more at aka.ms/hybridcloudgovernance

About the Analysts

Carla Arend, Senior Program Director, Lead Analyst, Cloud in Europe, IDC

Carla Arend is a senior program director with the European software and infrastructure research team and heads up IDC's European cloud research. She provides clients with key insight into market dynamics, vendor activities, and end-user adoption trends in the European cloud market.

Ralf Helkenberg, Research Manager, European Privacy & Data Security

Ralf Helkenberg is research manager for IDC's European Security group with a focus on European Privacy & Data Security. His research covers the evolving EU data privacy and cybersecurity regulatory landscape, and the market dynamics and technology developments within privacy compliance, de-identification and data security.

Denis Maslennikov, Senior Research Analyst, Cloud Security

Denis Maslennikov is senior research analyst for IDC's European Security group. Previous work experience includes working for Adaptive Mobile Security and Kaspersky Lab where he was responsible for mobile malware research, mobile spam analysis and research into specific threats in mobile security.
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.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters
5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.