00.00.00

Velotix

LEGACY TO LIFTOFF:

WHY NOW'S THE TIME FOR CLOUD-BASED GOVERNANCE

WWW.VELOTIX.AI

EXECUTIVE SUMMARY

Some people theorize that the phrase “cloud computing” was coined back in 1996. If this is true, cloud computing would be a Generation Z twenty-something today. And because of that, yet to reach maturity in terms of widespread adoption and implementation.

According to a key survey of North American tech executives, 52% choose to run more than half of their workloads and applications on-premises. For respondents working in finance, the figure goes up to 55%. Among those working in government, 100% have over half their applications on-premises. Some of the reasons given include a lack of budget, tools, or cloud-based skills or expertise.

Within the findings, there’s strong recognition that modernizing is crucial to success.

But data governance teams face a growing to-do list that can leave cloud on the back burner. The way data is collected and stored is evolving, and bringing new risks along with it. Data is coming from omnichannel sources, in unprecedented volumes, and at greater velocities.

Amid such huge growth, they’re also tasked with making the data available for analyzing, visualizing, and decision-making. While also making sure access is compliant with the growing number of privacy and protection regulations from governments. These are part of a global trend, with Gartner predicting that

> 75% of the world’s population will have itspersonal data covered under modern privacy regulations by 2025.

Note that covered won’t always mean protected. That’s up to organizations, who must identify the tools and platforms to secure data and provide access to insights. However, many face obstacles in the form of legacy infrastructure. Designed in an era before modern data regulations, these systems often limit the ability to adapt and unlock the cloud’s business potential.

For organizations looking for ways to catch up and compete in the cloud, here’s the good news: It is possible to migrate your workloads while providing compliant data access to the business. Even when operating in highly regulated industries that require specific policy controls. This eBook will share some of the ways it can be done.

YOU'LL FIND FOUR SECTIONS:

ONE

Monolithic mainframes and talent shortages Discover the drivers that have led to the current challenges

TWO

Why organizations should move to the cloud View some of the benefits of a compliant cloud

THREE

Barriers to cloud migration Find out the impact on compliance and governance

FOUR

How to remain compliant in the cloud Explore a data policy plan for control, compliance, and complexity

MONOLITHIC MAINFRAMES AND TALENT SHORTAGES

In the study cited above, almost four in five (79%) cite legacy applications as blockers to achieving digital transformation. Often monolithic and written for older or now-obsolete platforms, these apps are hard to decouple and turn into layers or components – a process which is essential for migrating to the cloud.

A negative cycle can then appear. It's harder to make log files from legacy systems, which makes it difficult to meet modern expectations around audits, visibility, and traceability.

Naturally, there's also an element of "if it isn't broken, don't try to fix it" when sticking to mainframe systems, some of which date back to the 1970s. Especially for governance teams operating in strictly regulated industries.

The potential information security risks of migration can appear to outweigh the perceived benefits. In this scenario, mitigating risk may be the immediate challenge.

However, it may not be sustainable.

After all, maintaining legacy systems calls for legacy knowledge. Many environments are built and run on the programming language COBOL, born in 1959, and are often incompatible with modern cloud solutions.

Talent is already at a premium, and increasingly likely to be focused on cloud-native environments and app development. Finding qualified professionals prepared to work with older systems, rather than newer technologies, is only going to become more difficult.

Over time, maintaining legacy systems without the necessary expertise may present a bigger risk to business security and viability.

THE FUTURE OF DATA GOVERNANCE: OBSERVATIONS FROM MAJOR ANALYSTS

Further risk comes from losing the data-driven insights required to compete.

Consider how many institutions are now focusing on enriching data that arrives unstructured, semi-structured, structured, machine-generated, and via streaming services.

This represents a shift in focus, which Gartner has described as "from big to small and wide data." The analysts expect the shift to be realized by 2025, with greater visibility, robustness, and insights extracted from platforms, applications, and AI.

Alongside building new business models and growth opportunities, this form of distributed data requires a similarly transformative form of governance. One that's conducted in a way that allows policies to adapt to new regulations, stay compliant, and remain accessible to the right people. The process is becoming more complex, as more countries and regions adopt and update data privacy legislation.

It's also a business imperative – and a leading driver of data privacy investments, as detailed in the Cisco 2023 Data Privacy Benchmark Study. Among the list of benefits and ROI, respondents cite increased loyalty and trust, mitigating security losses, and improved agility and innovation.

Corporate reputation is a key consideration too. A McKinsey report highlights the concept of "digital trust" and how "many will take their business elsewhere when companies don't deliver it." Meanwhile, Gartner points to "increased consumer demand for subject rights and raised expectations about transparency."

It's clear cloud-based compliance can be a source of competitive advantage. It's also clear the cloud approach goes hand in hand with ensuring data privacy. Against a backdrop of many competing drivers and influences, let's break things down into three clear areas. The case for migration, the barriers and risks, and how to be compliant.

WHY ORGANIZATIONS SHOULD MOVE TO THE CLOUD

Beyond the well-documented advantages of cloud migration, there are specific advantages from a compliance point of view:

Achieving cost saving

You don't have to look far to find examples of large data breach fines, many involving high-profile brands. Along with reducing potential pay-outs, other savings can come from spending less time on manual processes and maintaining data centers and infrastructure. From a budget point of view, moving to cloud-based operations makes investment more predictable, without the larger initial expense that comes with capital expenditure.

Accelerating time to market

Consider manual forms of data governance, where access requests can sometimes take weeks to be approved. Insights are often out of date by the time they're available to those making requests. Harnessing cloud-based anytime anywhere access (with the correct controls) puts data at employees' fingertips.

Future-proofing enterprise data estates

When data governance can provide insights quickly, there is a much bigger opportunity to make informed business decisions at the right time. Cloud supports improved performance by separating storage and compute environments, making services – plus policy enforcement and access authorizations – easier to scale.

Improving security and compliance postures

The variety of incoming data privacy regulations means organizations are in a race to update data access policies. Cloud solutions can reduce the time it takes to make such updates, and also enable organizations to automate and scale policy updates.

Leveraging expert partnerships

Established market leaders can connect with agile third-party innovators – ones who might otherwise have been unwilling or unable to integrate with the market leaders' legacy infrastructure – to provide new products and boost customer experiences.

THREE COMMON PATTERNS FOR CLOUD MIGRATION

Balancing privacy with agility means multiple migration decisions. There's the scoping of architecture, identifying where and how much to integrate, moving the workloads from on-premises to cloud, and then validating the outputs.

There are three broad approaches to this, shaped by level of cloud maturity, the prevalence and state of legacy systems, and past strategies:

- **Full Migration**
  For new market entrants and startups, the all-in cloud-first approach can be relatively easy to achieve. For market-leading enterprises with long-established IT footprints, it's a different picture, usually involving vast resources and longer time frames.

- **Full Migration**
  Through mergers and acquisitions, some organizations fall into this approach by default. They end up taking on existing clouds, often from different providers, with the goal of consolidating departments.

- **Hybrid approach**
  Hybrid has the added advantage of preserving valuable IP built up over years of business rules. Plus there's a high probability that employees are already using Microsoft 365 and other cloud-based apps, making behavioral change easier to effect.

BARRIERS TO CLOUD MIGRATION

Organizations cite a variety of reasons for delaying cloud migrations. Banks and long-established financial institutions in particular face unique challenges, owing to their legacy-led landscape. Below are some of the common issues:

Technical debt

Legacy systems often mean lots of lines of complex code. Combine these with non-standardized product purchases, often made over many years. Then add in data stored in often-siloed repositories.

The result is an environment where it's difficult to repurpose and rewrite for the cloud. After all, database infrastructure is a long way away from cloud infrastructure. Organizations then face a form of "software debt" or "technical debt".

To help solve technical debt, companies could migrate their existing apps to a virtualized cloud environment. Although this "lift and shift" approach often means losing out on many cloud-based benefits, and is likely to require additional security.

An alternative is refactoring for the cloud, but that often requires modernizing core banking applications, with potential downtime impacting day-to-day operations.

Fear of failure

There are many reasons why a reported 70% of transformation projects fail. Organizational hierarchies and structures can oftentimes have a negative impact.

That's because they're typically built for applying top-down approaches. This rarely works with transformation projects that require behavioral change across silos. Instead, disconnects can soon appear between strategy and execution.

It's likely that many members of the team have gone through previous migrations and transformation programs. Some will have experienced "cloud bill shock", where, instead of savings, teams are caught off guard by an unexpected overspend on their cloud bill. That elastic pay-as-you-go pricing may have sounded great – until the bill comes in for a resource-hungry virtual machine that someone spun up and forgot about.

Non-compliance risks

Migrating to the cloud also means evaluating how regulations translate to the cloud, and where responsibilities and boundaries appear. For example, a cloud provider may have cloud architects who require privileged access to data; organizations must consider how they can allow this without compromising security or data protection.

At the same time, the business also has obligations to control data collection and maintain its data, alongside defining the types of metadata to be collected and used.

Cloud is also a driver for updated regulations, such as PCI DSS. An updated version of the payment card standard was released in 2022, and includes stipulations for providers to define “controls so that each customer can only access their own environment.” Merchants have until 2024 to get their access controls updated and compliant.

Difficulties with deployment and decoupling

Migration can mean decoupling workloads from infrastructure, with responsibilities spread between cloud providers and SaaS vendors. This opens up new challenges around following the Principle Of Least Privilege, with increasing numbers of users and third parties requiring access.

Teams with expertise in legacy and on-premises infrastructure have to identify the right partner to ensure enhanced security and privacy for data “in transit.” It’s a long way from simply adding more physical hard drives and scaling on-premises.

More flexibility, less visibility

The move from physical locations to virtualized environments means enterprises have to find new ways to maintain visibility of where data resides in the cloud. There’s constant pressure to make sure they’re within localized and industry-specific regulations.

With multi-cloud environments, these challenges are multiplied, with different providers having different identity policies, access controls, and permissions.

HOW TO REMAIN COMPLIANT IN THE CLOUD

For other organizations yet to start their cloud journey, the clock's ticking.

By 2025, 85% of organizations are forecast to be cloud-first.

Combine this adoption with the global rise in data privacy regulations, and organizations have to start accelerating their progress.

Alongside knowing where data is located, organizations also have to know – and be able to show – data classifications, control types, and monitoring strategies. It then becomes possible to catalog and tag the data correctly.

Organizations are now seeing success from implementing cloud migrations and harnessing transformative technologies. Common themes are beginning to emerge, such as centralized control for distributed access. Automation is bringing down the time taken for data access decisions from weeks to minutes. Symbolic AI is being deployed, improving accuracy and making it easier to apply data policies.

The rich potential is why it's a case of when, and not if, cloud migration will become central to the future of data governance. With that in mind, here's how to stay compliant in the cloud.

SIMPLIFY ACCESS CONTROLS

Switch to a centralized platform, and data access and governance becomes finely grained. Risks from multiple data sets, such as errors, breaches, or duplication, are mitigated. Managing access through a single pane of glass makes it easier to adopt zero-trust policies.

The increased visibility also helps to answer one of the biggest concerns around cloud migration – the potential loss of control to a third-party provider.

It then becomes possible to quickly answer four key access control questions:

1. **Who and what roles have access to sensitive data?**
2. **What types of sensitive data has been accessed?**
3. **What sensitive data sources are accessed most often?**
4. **Which users have the highest sensitive data exposure?**

To scale this sort of knowledge, policies must be written in plain English that non-technical users can understand. This also supports data stewards, who play a crucial role in managing data access locally.

Over time, organizational culture can become more data-driven and data-democratized. After all, modernization isn't just an IT responsibility – it benefits the entire business.

REVIEW ACCESS CONTROL TYPES

Assigning access based on combinations of attributes makes access more dynamic, but organizations still need to be able to consistently apply their policies on a large scale.

To keep things consistent and standardized, choose a centralized platform. This means policies can be applied across multiple cloud environments, identifying sensitive data using advanced analytics that enrich data with auto-tagging cataloging.

There's also the added advantage of centralizing reporting. Alerts and exceptions can be viewed from one dashboard, enabling a single source of truth.

CENTRALIZE POLICY MANAGEMENT AND MONITORING

Assigning access based on combinations of attributes makes access more dynamic, but organizations still need to be able to consistently apply their policies on a large scale.

To keep things consistent and standardized, choose a centralized platform. This means policies can be applied across multiple cloud environments, identifying sensitive data using advanced analytics that enrich data with auto-tagging cataloging.

There's also the added advantage of centralizing reporting. Alerts and exceptions can be viewed from one dashboard, enabling a single source of truth.

AUTOMATION IS THE ANSWER

As data sources and volumes continue to grow, it's time to automate data management. Your chosen data management platform must offer automation across:

- **Data discovery and classification**
  Automatically detect, classify, and tag sensitive data and PII
- **Policy enforcement**
  Make use of existing data catalogs to sync and align metadata
- **Access monitoring**
  Ensure visibility of who's accessing data in real time, to gather insight on usage and adjusting based on exceptions
- **Activity logs**
  Track requested and actual changes made to logs, with alerts to support permissioning to users without unnecessary delays
- **Audit logs**
  Policy-related events should be automatically logged, with end-to-end data lifecycle transparency for auditing

PLOTTING THE PATH TOWARD CLOUD-BASED DATA GOVERNANCE

It's clear there are many moving parts for cloud-based data storage and management. Employees will change roles and companies, limiting the effectiveness of role-based data access.

There's the constant growth in data flowing into the enterprise, much of it unstructured. Plus the many new laws and directives set to be enacted, along with updates to existing data privacy regulations.

That's why modernization and migration has to start from the core. Where the foundation is a centralized data security platform, offering a single pane for managing today's complex data landscape. Supported by metadata, tags, and catalogs to make access granular and contextual, far beyond roles or rows and columns.

Automation brings further efficiencies across data discovery, classification, and the protection of sensitive information. This frees up the human-in-the-loop for managing alerts, processing edge cases, and configuring exceptions.

Meanwhile, symbolic AI can be introduced, learning from policy decisions and improving actions for the business in real time. The complexity of policies is matched by the intelligence of the platform, capable of considering who gets access, when, where, how, and for what purpose.

Although that type of AI is only available from one particular provider: Velotix. Contact us to find out how Velotix can support your cloud-based governance. Whatever stage of migration you're at, we can help you take the next step in your journey.

OUR MISSION

TO ENABLE THE SECURED, EFFICIENT, AND COMPLIANT USE OF DATA.

Velotix

WWW.VELOTIX.AI