ISG Provider Lens™

Multi Public Cloud Services

Sovereign Cloud Infrastructure Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

aws

QUADRANT REPORT | DECEMBER 2023 | EU

Table of Contents

Report Author: Rohan Thomas

Localized data residency is a key priority for sovereign cloud services providers

The Gaia-X initiative is a comprehensive framework designed to govern the data sovereignty of information deemed confidential by EU member states. The initiative has grown from 22 European stakeholders since its launch in 2019 to over 340 organizations as of 2023. While stringent security and encryption are integral to the framework, Gaia-X has also called for data residency inside the EU and recommended that an EU entity hold 50 percent of the total ownership stake in the sovereign cloud service. Gaia-X serves as a compass for our research on the sovereign cloud quadrant.

In April 2022, Gaia-X proposed categorizing the sovereign cloud service providers under three labels. While Labels 1 and 2 had standards of cybersecurity and interoperability far superior to those inherent in other public cloud service offerings, Label 3 stressed European ownership.

The recommended framework suggests that having European control over the provider of sovereign cloud services would increase the privacy, security, and confidential of data considered sovereign by the EU. However, this has created obstacles for EU organizations, both governmental and commercial, in maintaining a continuous service flow from their chosen providers. These organizations still depend on the scalability and comprehensive technology stack that the global hyperscalers – AWS, Microsoft, and Google – offer and continue to develop.

Consequently, the framework serves as a blockade to EU entities that want to access a more agile, automated, and scalable platform but cannot due to data privacy requirements. Cloud service providers, both within the EU and outside, continue to work extensively with key stakeholders to develop a seamless process that adopts a highly scalable cloud ecosystem. This process is aimed at cultivating a highly scalable cloud environment, built upon sophisticated technology and leveraging open-source platform, ensuring interoperability with a strong emphasis on EU standards.

Hyperscalers who provide **sovereign services** but are **not EU-based** have a **complex GTM**.

An emerging key trend is the formation of partnerships between European service providers and global hyperscalers. Through such partnerships, European service providers can provide hyperscale-grade sovereign cloud services and yet comply with EU and regional security and ownership norms. Google Cloud seems to be a frontrunner in such partnerships. As of 2023, the company partners with T-Systems and Thales (jointly created S3NS) to extend its hyperscale-grade sovereign services to European institutions. Additionally, in March 2023, Google announced its partnership with Proximus to provide sovereign services to customers in Belgium and Luxembourg.

Another reason behind such partnerships is to alleviate European companies' concerns about the potential data hack by foreign government entities. The Clarifying Lawful Overseas Use of Data (CLOUD) Act is a notable example of such foreign interference in the data privacy of entities inside the European Union. Enacted in 2018 by the US government, the Act mandates that US-based technology companies provide data stored on their servers, including overseas data, to federal law enforcement agencies when presented with a warrant.

Given the stringent data residency regulations, the European Commission insists on creating a separate pool of sovereign cloud data centers with physical guard rails. This arrangement prevents sovereign data from residing in data centers consisting of components from manufacturers whose security is not robust or does not comply with those set forth by the European Commission.

The following factors are expected to strongly influence the sovereign cloud market in the EU.

1. **Cybersecurity and encryption:** Enhancing sovereign data security will be key. This will involve ensuring personnel who handle sovereign data are at least based in the EU, although EU citizens are preferred. Strong data encryption is required in every phase of the data lifecycle, including at rest, during computation, and in transit between EU and non-EU countries or within EU member states. External key management solutions are emerging as an important feature companies will leverage. Encrypted keys configured by the companies are opaque to everyone else. This ensures that access rights to sovereign data are further curtained from the personnel of the cloud service provider.

2. **Physical guardrails:** This follows up on the enhanced security requirements for sovereign cloud. Gaia-X recommends that infrastructure in which sovereign data is stored be isolated from other public cloud infrastructure. Identifying sovereign data from a data pool, storing it in isolated centers and reintegrating some of it substantially challenges service providers' technological capabilities.

3. **Partnerships and alliances:** Although there are a large number of European cloud service providers, the scale of their data center ecosystem and its technological capabilities are not as attractive as that offered by global hyperscalers. Observers can expect further tie-ups between local and global players to meet end users' expectations for hyperscale-grade sovereign services. Complexities will, however, arise while establishing such partnerships from a policy-making perspective and on a technical level. The former will include enforcing European ownership, localized administrators, and immunization of the sovereignty of EU data from foreign legislation that may delegitimize it. Technical complexities will include not only enforcing physical guardrails to infrastructure of the global hyperscale in which sovereign data is stored but also segregating data based on its sovereignty and enforcing different governance policies. Due to the inherent complexities associated with implementing sovereign data services, it is likely that providers of cloud consulting and managed services will partner with European service providers of public cloud infrastructure.

4. **Incorporation of open-source technologies:** Providers of sovereign cloud services must negate the probability of vendor lock-ins for their sovereign cloud

data services. There will be a growing need to incorporate container-based and open-sourced technologies to create an agile application that can easily integrate with other (including hyperscale) environments to maximize interoperability. Membership in not-for-profit organizations such as the CNCF will enable cloud service providers to adopt cloud-native technologies that are more innovative and agile to their sovereign cloud requirements.

5. **Industry-specific sovereign cloud services:** Many companies in the EU have expressed interest in incorporating sovereign cloud capabilities into their infrastructure. A sizable number of these companies have begun the groundwork in identifying their sovereign cloud service requirements. The number of such companies is expected to swell in the near future. Sovereign cloud service providers should standardize the governance policies based on the industry vertical of the respective customer.

Partnerships and alliances between European service providers and global hyperscalers will be a key theme in the market. Additionally, sovereign cloud providers will collaborate with providers of public cloud managed services to improve the implementation of sovereign cloud services.

Provider Positioning

Page 1 of 2

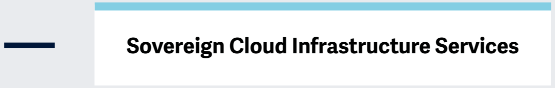
	Sovereign Cloud Infrastructure Services
3DS outscale	Product Challenger
AWS	Leader
DATAGROUP	Contender
Google	Leader
IONOS	Contender
Microsoft	Leader
noris network	Contender
Oracle	Product Challenger
Orange Business	Leader
OVHcloud	Leader

Provider Positioning

Page 2 of 2

	Sovereign Cloud Infrastructure Services
plusserver	Contender
Scaleway	Contender
STACKIT	Contender
Swisscom	Contender
Tietoevry	Contender
T-Systems	Leader

This study focuses on what ISG perceives as most critical in 2023 for **Multi Public Cloud Services**.



Sovereign Cloud Infrastructure Services

Simplified Illustration; Source: ISG 2023

Definition

This study assesses providers offering public cloud services, including consulting and transformation, managed services, public cloud infrastructure, FinOps and other services. Providers in scope leverage automation tools to effectively manage, secure and optimize public cloud infrastructure.

In recent years, there has been rapid growth in public cloud adoption as part of digital transformation engagements. The many benefits of the public cloud surpass on-premises infrastructure in several ways, making it the preferred choice for greenfield infrastructure operations and application development in most cases. Other key reasons for this preference stem from a heightened focus on cybersecurity, a greater push toward IT cost optimization and operational efficiency, and the increased deployment of automation tools for efficient data management, along with driving sustainability initiatives by leveraging cloud infrastructure.

Enterprises continue to seek strategic providers that facilitate cloud transformation engagements on major hyperscalers such as AWS, Microsoft Azure and Google Cloud. The service providers will not only continue to manage the workloads on an ongoing basis but also assist enterprises in controlling, optimizing and managing cloud expenses through FinOps strategies.

With enterprises realizing that the lift and shift migration strategy does not provide the benefits expected from public cloud, they are on the lookout for providers that can help accrue the complete potential of cloud technology. With this, we will be seeing an increased demand for re-architecting workloads and leverage cloud-native technologies for their migration engagements. Also, in the coming years, enterprises are likely to take a conservative approach to spending on public cloud infrastructure. The increasing adoption of FinOps strategy will support this approach and enable the optimization of cloud resources and, consequently, reduce cloud consumption and cloud bills.

Scope of the Report

This ISG Provider Lens™ quadrant report covers the following one quadrant for services/solutions: Sovereign Cloud Infrastructure Services.

This ISG Provider Lens™ study offers IT decision-makers:

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments (quadrants)
- Focus on the regional market

Our study serves as the basis for important decision-making by covering providers' positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing vendor relationships and potential engagements.

Provider Classifications

The provider position reflects the suitability of IT providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions IT providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between $20 million and $999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).

Provider Classifications: Quadrant Key

Product Challengers offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not in means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.

Sovereign Cloud Infrastructure Services

Who Should Read This Section

This report is relevant to enterprises across industries in the EU and will help them evaluate providers of sovereign cloud infrastructure services in the multi public cloud environment. In this quadrant report, ISG defines the current market positioning of service providers in the EU and shows how they address the key challenges that confront enterprise clients in the EU.

Enterprises emphasize that providers focus on adherence to strict data residency regulations, and the European Commission advocates the establishment of dedicated sovereign cloud data centers equipped with stringent physical security measures. This setup ensures sovereign data is not stored in data centers that use components from manufacturers with inadequate security measures or those that fail to meet the European Commission's compliance standards.

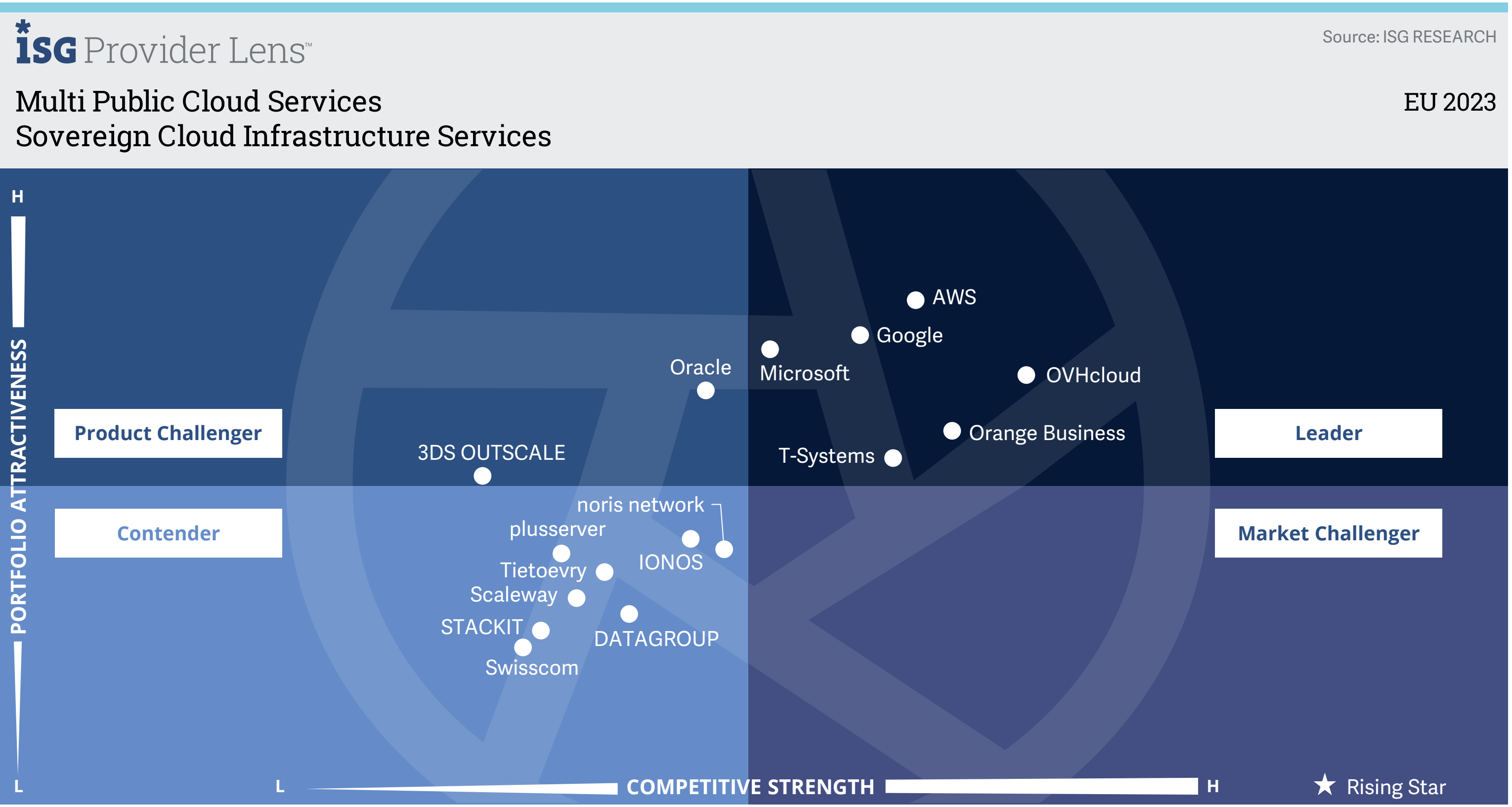
Enterprises in the EU are looking for providers that engage with the Gaia-X initiative to support the implementation of sovereign cloud services designed to align networks across the region, thus ensuring trust and data security under the concept of privacy by design. It effectively serves as a blockade to EU-based institutions that want to access a more agile, automated, and scalable platform but are hindered by data privacy requirements.

ISG notes a growing number of partnerships between European service providers and global hyperscalers to provide hyperscale-grade sovereign cloud services that comply with EU security and data ownership norms. Providers are enhancing their encryption and key management capabilities in every phase of a data cycle, ensuring access rights to sovereign data are denied to the personnel of the cloud service provider.

IT leaders should read this report to better understand the relative strengths and weaknesses of sovereign cloud infrastructure service providers and learn how their approaches to the market can impact enterprise public cloud strategies.

Software development and technology leaders should read this report to understand the relative positioning and capabilities of sovereign cloud providers that can help them procure infrastructure and platform services to migrate their workloads to public cloud platforms.

Sourcing, procurement and vendor management professionals should read this report to better understand the current landscape of sovereign cloud infrastructure service providers in EU.



This quadrant assesses service providers **who provide IaaS that are sovereign per the Gaia-X** framework. Most of the service providers covered in this quadrant have **European heritage** and have **data residency within the EU**.

Rohan Thomas

Definition

This quadrant assesses providers that offer secure cloud infrastructure designed for hosting enterprise and public sector workloads and data considered "sovereign." Clients consume infrastructure functionality as on-demand and web-centric services, with a portfolio of services including computing power, memory, storage, network, backup and container management functions.

The providers should offer a scalable, agile, flexible and secure cloud infrastructure that ensures data sovereignty. This means that sovereign data resides within data centers located in a specific geography and is subject to local jurisdiction. The providers must prevent access to sovereign data by foreign entities and protect it from potential cyber-attacks. The sovereign cloud architecture should adhere to specifications outlined by projects such as Gaia-X, GDPR, electronic data interchange (EDI) and more. The framework also advocates using open-source technologies such as OpenStack, Kubernetes and Terraform, reducing reliance on proprietary technologies and avoiding vendor lock-in, ensuring data accessibility. Sovereign cloud providers must establish measures to separate their clients' data from non-sovereign data within their data centers.

***Note:** Any cloud data center provider meeting the criteria specified below will be eligible to be rated in this quadrant. Also, for this year, this quadrant will be limited to EU exclusively.*

Eligibility Criteria

1. Data center infrastructure should be present within the **specific geography** and comply with **regional regulations**
2. Easy access, **transparent pricing** and support for consumption-based, reserved instance, and dedicated instance billing models
3. Compliance with **GDPR** for storing and processing personal data
4. Compliance with **certifications** including BSI-C5, PCI DSS, ISO 27001, ISO 20000, EN 50600, TÜV IT Level 4, KRITIS, HDS and HIPAA
5. Offer **interoperability** with standardized interfaces and avoid vendor lock-in
6. Robust **security** measures with strict access controls
7. Infrastructure **architecture** is designed to comply with **governance** and **compliance** regulations to secure data and applications
8. Incorporate **open-source** technology components in the **architecture** and **design** of sovereign cloud
9. Implementation of **sustainable initiatives** to provide stable and long-lasting software infrastructure
10. Leveraging **encryption** and **cryptography** to protect the confidentiality and integrity of sovereign data
11. Monitoring and auditing to detect and respond to any security threats or incidents

Observations

The quadrant covers global hyperscalers and EU-owned cloud service providers. OVHcloud has a competitive edge in the market because of its extensive regional coverage, attractive pricing models and brand credibility. While OVHcloud does have a host of technological capabilities ranging from agile container-based technologies to high-performance instances, its portfolio is not as attractive as that of the world's leading hyperscalers – AWS, Google Cloud and Azure.

Although they are prominent in the market, the competitive strength of the hyperscalers is not as much as the other participants that have been identified as market leaders. This is primarily because of their non-European heritage. Google Cloud's go-to-market (GTM) strategy of partnering with European cloud service providers has helped it extend its cloud services to encompass data sovereignty.

In terms of portfolio attractiveness, AWS ranks the highest. Its technology stack built from the ground up is extensively leveraged by companies to design, build and manage an agile and secure public cloud infrastructure. AWS's "sovereign by design" feature provides end-users with a highly secure cloud environment.

AWS continues to invest in its product development for the sovereign cloud. In August 2023, AWS announced AWS Dedicated Local Zones. Then in October 2023, the company announced the launch of its AWS European Sovereign Cloud. Together, AWS is expected to enhance the degree of compliance it can offer for customers from highly regulated industries in the EU in the future.

From the 50 companies assessed for this study, 16 qualified for this quadrant, with six being Leaders.

aws

AWS has the AWS Nitro System as the foundation of its sovereign cloud services. The system is highly secure and can spin up instances quickly. AWS' external key store feature enhances encryption strength. Multiple availability zones further strengthen resilience.

Google

Google Cloud's GTM strategy of partnering with several local service providers has enhanced its reach among companies that require hyperscale-grade sovereign cloud services. Google's investments in GenAI improve automation and cybersecurity for these companies.

Microsoft

Microsoft encrypts sovereign data at rest, in transit and during computation. Its vast availability zones across 35 countries offer a scalable cloud environment with diverse data residency options.

orange™ Business Services

Orange Business provides flexible and agile software defined networking (SDN) capabilities for the sovereign cloud. The company's sovereign cloud solution is built using VMware's sovereign cloud stack. It does not leverage instances from AWS, Azure or Google Cloud.

OVHcloud

OVHcloud has a vast network of data centers both within and outside the EU. It is compliant with regional accreditations such as CISPE and SecNumCloud. The company's encryption is strong and it provides key management services to limit admin access.

T-Systems

T-Systems has partnered with Google Cloud to provide hyperscale-grade sovereign services to customers primarily from the DACH region. The company has enhanced its partnership with UiPath to provide next-generation AI services to its sovereign cloud customers.

AWS

Leader

> "AWS' network of data centers across the EU provides sovereign cloud services that are highly scalable. The AWS Nitro System, the foundation of AWS' cloud services, ensures data residency, privacy, and sovereignty."
>
> *Rohan Thomas*

Overview

AWS is headquartered in Washington, U.S. and operates in 32 regions. In FY22 the company generated $80.1 billion in revenue. AWS has 8 regions in Frankfurt, Ireland, London, Milan, Paris, Stockholm, Spain, and Zurich; and more than 120 Content Distribution Network (CDN) points of presence in more than 25 cities across 19 European states. AWS has 4 Local Zones and also offers AWS Dedicated Local Zones. The company recently announced plans to launch the AWS European Sovereign Cloud, an independent cloud for Europe.

Strengths

Digital sovereignty by design: The AWS Nitro System is the foundation of AWS' sovereign cloud stack. The AWS Nitro System provides a strong physical and logical security boundary to enforce access restrictions so that nobody, including AWS employees, can access customer data running in Amazon EC2. The security design of the Nitro System has been independently validated by the NCC Group in a public report.

Strengthened resilience: AWS delivers its services through multiple Availability Zones (AZs). Clients can partition applications across multiple Azs in the same AWS region to enhance the range of sovereign and resilient options. AWS enables its customers to seamlessly transport their encrypted data between regions. This ensures data sovereignty even during geopolitical instabilities. AWS also allows its customers to enforce stringent guardrails to meet local data residency requirements via the AWS Control Tower.

Encryption everywhere: AWS offers the capability to encrypt all customer data, whether in transit, at rest or in memory. Key Management Service (AWS KMS) is integrated with over 115 services. AWS KMS is designed so that no one, including AWS employees, can retrieve plaintext keys from the service. The AWS KMS feature, External Key Store (XKS), allows keys to be generated and stored in an external key manager outside of AWS.

Caution

The fact that AWS is an entity that is headquartered in the U.S. and operates in the European sovereign cloud space could prove to be complicated. Additionally, while AWS provides tools and solutions to facilitate interoperability, it tends to refrain from actively endorsing this capability.

Appendix

The ISG Provider Lens™ 2023 – Multi Public Cloud Services study analyzes the relevant software vendors/service providers in the EU market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research™ methodology.

Lead Author:
Rohan Thomas

Editors:
Kondappan S and John Burnell

Research Analyst:
Manoj M

Data Analysts:
Sachitha Kamath and Lakshmi Kavya Bandaru

Consultant Advisor:
Susanta Dey

Project Manager:
Manikanta Shankaran

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research™ programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of November 2023, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars ($US) unless noted.

The study was divided into the following steps:

1. Definition of Multi Public Cloud Services market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
   * Strategy & vision
   * Tech Innovation
   * Brand awareness and presence in the market
   * Sales and partner landscape
   * Breadth and depth of portfolio of services offered
   * CX and Recommendation

Author & Editor Biographies

Author

Rohan Thomas

Senior Lead Analyst

Rohan Thomas has nearly a decade's worth of knowledge expertise in the realms of ICT, which include telecommunications, data centers, and networks and application performance management. At ISG, Rohan is the lead analyst for ISG Provider Lens™, leading research activities and benchmarking exercises pertaining to the regional adoption of digital infrastructure such as private/hybrid cloud.

He has a Bachelor's degree in Mechanical Engineering from Visveswaraya Technological University and a Master's degree in Computer Aided Design and Manufacturing from Vellore Institute of Technology.

Enterprise Context and Overview Analyst

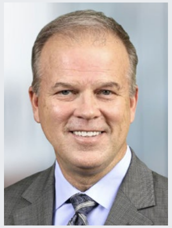
Manoj M

Research Analyst

Manoj is a research analyst at ISG and supports ISG Provider Lens™ studies on Private/Hybrid Cloud – Data Center Services, Mainframes, Cloud Native Services & Solutions and Public Cloud Solution and Services. He also supports the lead analysts of multiple regions in the research process. Prior to this role, he supported the ROI process in sales intelligence platform and was an individual contributor in handling research requirements for advanced technologies in different sectors.

He has considerable expertise in predicting the automation impact by considering certain parameters such as productivity, efficiency and time reduction. During his tenure, he has supported research authors and authored Enterprise Context and Global Summary reports with market trends and insights.

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

About Our Company & Research

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens™ research, please visit this webpage.

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit isg-one.com.

DECEMBER, 2023

REPORT: MULTI PUBLIC CLOUD SERVICES