

Portability and Interoperability

In the event of service disruption, data portability and application or service interoperability can enable organizations to take advantage of the technical solutions and contingency arrangements that are necessary for returning to normal operations. These features foster resilience by allowing customers to operate across different services and contract with multiple cloud providers. As a result, although they serve different functions, portability and interoperability are often spoken of together.

Key Considerations

- **Deficient standards and adaptation tools.** Existing standards and adaptation tools (for example, protocol converters, translators, and software environment emulators¹) for portability and interoperability are insufficient to enable the amount of flexibility enterprise customers desire and to fully offset the threat of service disruption. This prevents the creation of adequate approaches to enabling the exchange and migration of cloud-hosted data and/or applications. Moreover, a prolonged transition period will ensue before adequate standards and adaptation tools gain significant market presence, further delaying efforts to mitigate service disruption challenges.
- **Portability is difficult to operationalize.** Even if cloud providers enable and support greater portability, customers must make significant time, training, and financial investments (for example, purchasing duplicate software licenses) to successfully move workloads between cloud environments. Moreover, even if they can make these investments, they may need to convert the data to other formats (to be compatible with the new environment) and ensure that the same identity, security, and privacy management policies apply in this new environment.² These factors prevent organizations from rapidly moving data in response to an incident.
- **Barriers to interoperability.** Interoperability requires much deeper technical integration and data and IP sharing among cloud providers, which they may resist. Moreover, there might be relatively less customer demand for interoperability, as portability seems to provide much of the flexibility and agility that customers seek.
- **Interoperability can expose customers to security risks.** Although, on balance, relying on multiple cloud providers seems to reduce the risk of service disruption and data loss, this also increases the surface area of a customer's system and the probability of exposure to individual security vulnerabilities. Moreover, their dependence on additional cloud providers and other third parties complicates efforts to understand, model, and bound their risk profiles, as customers will be concerned about end-to-end security while each provider might only seek to secure its offering.

- **Emergence of specialized providers.** Greater portability and interoperability may diminish an individual provider’s revenue.³ As a result, at least some providers might not support efforts to increase and expand these capabilities. However, as customer demand for portability and interoperability increases, a range of specialized providers are emerging to fill this gap, enhancing growth in the overall cloud services market.
- **Shared responsibilities when transferring data.** There are multiple parties involved in the transfer of data, and as a result, they share many responsibilities for maintaining the security and privacy of the data as it migrates from one environment to another.⁴ These parties, especially customers, may not always be aware of or understand their responsibilities.

Stakeholder Perspectives

Government	Providers	Customers	Others
<ul style="list-style-type: none"> • Seek assurance that government functions and the broader economy can expect continuous and reliable service across providers by creating or encouraging the development of standards for interoperability and portability. 	<ul style="list-style-type: none"> • Resist or avoid requirements for portability and interoperability that may affect the security (real or perceived) of their products and erode their market share. 	<ul style="list-style-type: none"> • Seek to acquire or retain the ability to easily switch or interoperate between cloud providers and port data in order to safeguard their businesses and restore service functionality in the event of cloud service disruption. • Worry about losing the benefits of the native cloud environment when designing and operating to optimize portability. 	<ul style="list-style-type: none"> • <i>Insurers:</i> May be interested in requiring portability, interoperability, and multi-cloud arrangements as a condition for providing coverage.

Tensions with Other Cloud Governance Issues

- **Incident Handling Procedures** and **Data Retrievability and Backup Arrangements:** The inability to port or interoperate workloads between different cloud providers’ services may slow or prevent efforts to restore service in the event of cloud outage. It may also

make data retrievability arrangements less useful, if backup data and workloads cannot be transferred to functioning cloud environments.

- **Effects of Cloud Market Concentration:** Portability and interoperability could increase competition between cloud providers, potentially helping consumers and enterprise customers access higher-quality cloud services in a more cost-effective manner. Yet many cloud providers' business practices increase customer dependence on a single provider, exacerbating the consequences of business disruptions and other failures.⁵ This lack of portability and interoperability could worsen the consequences of large-scale disruptions, especially if they affect multiple hyperscale providers.

Potential Ways Ahead

Government

- Encourage the use of hybrid and multi-cloud strategies to decrease disruption risks.⁶
- Encourage agreement on common terminology and principles for portability and interoperability in consultation with providers and customers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,⁷ IEEE's P2301/P2302,⁸ and ISO/IEC's 19941.⁹

Providers

- Develop and promote (in coordination with other providers) voluntary industry norms on portability and interoperability (for example, advancing a "customer bill of rights" for workload portability that includes technical and operational [licensing] standards and principles, such as a "transparency declaration,"¹⁰ to help customers understand available accommodations, which data can be imported and exported, as well as which data standards, formats, and file types are

Customers

- *Enterprise customers:* Those that are unable or choose not to adopt a multi-cloud strategy should use interoperability and portability tools to ensure continuity of business.¹⁵
- *Enterprise customers:* Encourage the development, promulgation, and use of adaptation tools (possibly created by third-party vendors).
- *Enterprise customers:* Encourage agreement on common terminology and principles for portability and interoperability in consultation with

Others

- *Third-party vendors:* Promote, create, and promulgate adaptation tools.

- recommended, used, or available).
- Encourage agreement on common terminology and principles for portability and interoperability in consultation with governments and customers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,¹¹ IEEE's P2301/P2302,¹² ISO/IEC's 19941.¹³ Develop appeals and complaint procedures¹⁴ whereby customers may raise concerns associated with (in)action by providers.
- Adhere to existing standards on open-source code and applications.
- governments and providers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,¹⁶ IEEE's P2301/P2302,¹⁷ and ISO/IEC's 19941.¹⁸

Recent Examples

- A recent survey commissioned by Google finds that only 17 percent of financial institutions have adopted a multi-cloud strategy, with 27 percent relying on a single cloud and 38 percent on a hybrid cloud architecture. "Notably, of respondents without a multi-cloud deployment, 88% reported they are considering adopting a multi-cloud strategy in the next 12 months." See: "[Google Cloud study: cloud adoption increasing in financial services, but regulatory hurdles remain](#)," Google Cloud, August 12, 2021 and "[Banks are moving their core operations into the cloud at a rapid rate. But new tech brings new challenges](#)," ZDNet, August 13, 2021.

- In Europe, the Gaia-X initiative aims to catalyze innovation by freeing customers from the business and security concerns associated with the dependence on a single cloud provider. Data interconnection is achieved through portability, which "ensures data and services from different sources can be easily exchanged within the digital infrastructure," and interoperability, which allows data services to be "transmitted seamlessly." See: "[GAIA-X: A Federated Data Infrastructure for Europe](#)," Gaia-x, n.d.

Notes

¹ Mark Jeffrey, "Interoperability and Portability in Cloud Computing," Microsoft, December 15, 2017, <https://blogs.microsoft.com/eupolicy/2017/12/15/interoperability-portability-cloud-computing/>.

² Lydia Leong, "Multicloud failover is almost always a terrible idea," Gartner (blog), October 14, 2021, https://blogs.gartner.com/lydia_leong/2021/10/14/multicloud-failover-is-almost-always-a-terrible-idea/.

³ Calls to increase interoperability across providers may challenge providers' business strategies, which often involve building customer dependence on their offerings.

⁴ Data Transfer Project, "Data Transfer Project Overview and Fundamentals," Data Transfer Project, July 20, 2018, <https://datatransferproject.dev/dtp-overview.pdf>.

⁵ OVH fire destroys one of its four data centers, rendering some services as "unrecoverable." See: Simon Sharwood, "OVH says some customer data and configs can't be recovered after fire, some seems to be OK, plenty is safe," The Register, March 15, 2021, https://www.theregister.com/2021/03/15/ovh_restoration_roadmap/.

⁶ These strategies can include arrangements for failover across regions, load balancers, application gateways, and more, and should as well include a complementary data backup strategy (for example, how frequent should the backup process be, how extensive, should they be simultaneous across all applications, and so on) and a strategy on how to address lost data. A disaster recovery plan should also account for the people, processes, and applications needed to restore functionality, and should be fully and regularly tested through disaster simulations.

⁷ "SWIPO (Switching Cloud Providers and Porting Data), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 'Porting of Data.'" See: SWIPO, "Switching & Porting," SWIPO, n.d., <https://swipo.eu/>.

⁸ Beyond Standards, "IEEE Addresses Standards for the Cloud," Beyond Standards (blog), IEEE Standards Association, April 18, 2011, <https://beyondstandards.ieee.org/ieee-addresses-standards-for-the-cloud/>.

⁹ “ISO/IEC 19941:2017 specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services. See: ISO, “ISO/IEC 19941:2017: Information technology – cloud computing – interoperability and portability,” ISO, December 2017, <https://www.iso.org/standard/66639.html>.

¹⁰ As advanced in the “Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services – CSP Transparency Statement,” SWIPO, May 27, 2020, <https://swipo.eu/wp-content/uploads/2020/10/SWIPO-iaaS-CSP-Transparency-Statement-version-2020-27-May-2020-v1.0.pdf>.

¹¹ “SWIPO (Switching Cloud Providers and Porting Data), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 “Porting of Data.” See: SWIPO, “Switching & Porting,” SWIPO, n.d., <https://swipo.eu/>.

¹² Beyond Standards, “IEEE Addresses Standards for the Cloud,” Beyond Standards (blog), IEEE Standards Association, April 18, 2011, <https://beyondstandards.ieee.org/ieee-addresses-standards-for-the-cloud/>.

¹³ “ISO/IEC 19941:2017 specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services. See: ISO, “ISO/IEC 19941:2017: Information technology – cloud computing – interoperability and portability,” ISO, December 2017, <https://www.iso.org/standard/66639.html>.

¹⁴ As advanced in the “Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services – CSP Transparency Statement,” SWIPO, May 27, 2020, <https://swipo.eu/wp-content/uploads/2020/10/SWIPO-iaaS-CSP-Transparency-Statement-version-2020-27-May-2020-v1.0.pdf>.

¹⁵ According to a 2021 report backed by Google, “Only 17% of the financial institutions surveyed . . . have already adopted multi-cloud as an architecture of choice, while 28% rely on single cloud.” Though, 88 percent of respondents without a multi-cloud strategy “reported they are considering adopting [one] in the next 12 months.” See: Zac Maufe, “Google Cloud study: cloud adoption increasing in financial services, but regulatory hurdles remain,” Google Cloud, August 12, 2021, <https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services> and Daphne Leprince-Ringuet, “Banks are moving their core operations into the cloud at a rapid rate. But new tech brings new challenges,” ZDNet, August 13, 2021, <https://www.zdnet.com/article/banks-are-moving-their-core-operations-into-the-cloud-at-a-rapid-rate-but-new-tech-brings-new-challenges/>.

¹⁶ “SWIPO (Switching Cloud Providers and Porting Data), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 “Porting of Data.” See: SWIPO, “Switching & Porting,” SWIPO, n.d., <https://swipo.eu/>.

¹⁷ Beyond Standards, “IEEE Addresses Standards for the Cloud,” Beyond Standards (blog), IEEE Standards Association, April 18, 2011, <https://beyondstandards.ieee.org/ieee-addresses-standards-for-the-cloud/>.

¹⁸ “ISO/IEC 19941:2017 specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services. See: ISO, “ISO/IEC 19941:2017: Information technology – cloud computing – interoperability and portability,” ISO, December 2017, <https://www.iso.org/standard/66639.html>.