Infosys® | CONSULTING

CLOUD CONTINGENCY FRAMEWORK

Travel Insurance for your Cloud Migration journey

An Infosys Consulting Perspective

By Shan Yong, Meghna Shekhar & Sachin Mahajan

Consulting@Infosys.com | InfosysConsultingInsights.com

INTRODUCTION

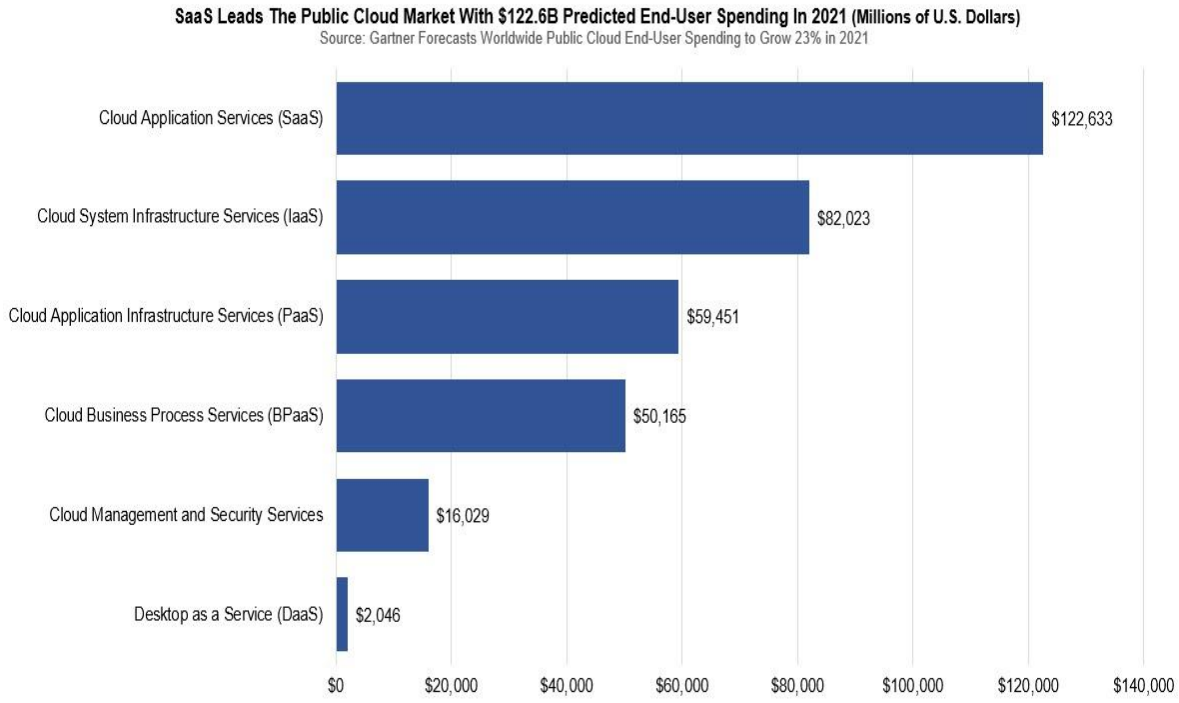
As the cloud Service providers have become more mature in their services and offerings, the chances of failure or disruption of services for the most prominent players in the market remain relatively low. Still, it's not unheard of.

While most organizations are aware of business continuity planning and disaster recovery and have mechanisms to effectively monitor the performance of applications deployed on the public cloud, very few organizations consciously and proactively monitor other risks categories like ethical, financial, competitive and legal, concerning their CSP.

It's now time for the organizations to be proactive in their approach and start defining a broader and more comprehensive public cloud exit strategy so they are well prepared for any contingency related to their CSPs.

CLOUD CONTINGENCY STRATEGY

According to Gartner, "Having a cloud exit strategy is like having a disaster recovery strategy: You hope you never need it, but you absolutely should have one to address cloud dependency risks".



As per Gartner's analysis, SaaS, and IaaS cloud lead end user spending in 2021 and will continue to do so in the near future.

As more and more organizations enthusiastically embark on public cloud adoption journey and move their business-critical applications on public cloud, there is a tremendous need for clear guidelines, processes, and customized roadmap to manage the risks in case of any adverse events taking place within the public cloud infrastructure, platforms, and applications. While most of these risk events can be managed and residual risks monitored, some of these events may require an organization to either partially or entirely exit from a public Cloud Service Provider (CSP). This is where the need to define a Cloud Contingency Strategy for an organization comes into play.

'Cloud Contingency Strategy' can be defined as the end-to-end process of identifying, monitoring, assessing, and addressing risks that could lead to a well-planned exit from IaaS, PaaS, and SaaS based CSP over a period.

WHY DO YOU NEED AN EXIT PLAN

The decision to exit a CSP may be based on one major event that has had a huge multi-dimensional impact on the organization's ability to deliver products or services or aggregation of smaller events over time, leading to an organizational consensus for an eventual exit.

While most of the global CSPs like Azure and AWS may have been stable historically, they are certainly not immune to outages or failures. Besides outages, there can be multiple other reasons for an organization to consider exiting from a CSP. Following are the key factors that are applied across organizations, geographies, and industries that could result in a cloud exit.

- **Regulatory changes & Compliance:** To be compliant to regulatory standards like CPS232-BCP, CPS-231-Outsourcing, CPS -220-Risk Mgmt., BS-11, GDPR, etc.
- **Ethical Issues with CSP:** Ethical issues with a CSP that are not aligned with organizational ethical standards.
- **CSP's financial viability:** A CSP may not have long-term economic viability to sustain, thereby potential to disrupt services in future.
- **End-User Satisfaction:** CSP offerings may not be aligned to the overall needs of the customers and may impact end-user satisfaction.

- **Gaining Stakeholders and Customer's confidence:** To assure availability and quality of service to the customers in the long run.
- **Unattractive Renewals:** Changes in CSP contract terms may potentially make a contract renewal unattractive for an organization.
- **Increased Costs:** CSP may decide to increase the costs of services, thereby leading to additional reoccurring expenses that may not be financially feasible.
- **Changes in Organizational Direction:** Changes in organization future directions and roadmap may impact the need for services from specific CSP.
- **Risk Reduction:** To manage the risk of utilizing public cloud for business-critical systems.
- **Service deterioration:** One or multiple aggregated instances of deterioration of cloud services.

WHO NEEDS A CLOUD CONTINGENCY STRATEGY

Every organization leveraging public cloud infrastructure must have a cloud contingency strategy. It may appear on the outset that a cloud contingency strategy may be limited to an organization with a colossal cloud footprint or for organizations where it gets mandated by regulations; however, the reasons for having a well-defined cloud contingency strategy goes beyond and above that and are applicable universally across geography and industry.

KEY FACTORS FOR A SUCCESSFUL CLOUD CONTINGENCY PLAN

While each organization may have different criteria for defining a successful cloud contingency strategy in line with its goal and larger business objectives, it must cater to the following critical factors while defining a cloud contingency strategy.

Well-defined Ownership:

A cloud contingency strategy is an enterprise strategy that cuts across multiple business units. A clearly defined ownership model is required for effective operationalization and governance.

Reuse, Enrich and Uplift:

Most organizations already have various tools and frameworks defined and operational. Therefore, a cloud contingency strategy should reuse, enrich, and uplift the existing frameworks with a cloud contingency lens rather than redefine something brand new.

Sustainable, maintainable, and usable:

Keep the cloud contingency strategy and framework simple, sustainable, maintainable, and usable updates regularly to retain relevance to the organization. It can be achieved through effective well-defined governance.

Data-driven decision making at the right level:

The decision should be driven by data points and consider all different aspects like risk level, impact, the timeframe of impact, organizational readiness, and viability for an exit, etc.

Decision at the right level:

Depending upon the type of cloud contingency scenario, the decision should be made at the right organizational level.

CRITICAL CORE ELEMENTS

The cloud contingency strategy must align to broader organizational goals and business objectives and align the core elements accordingly. However, as a best practice, several core elements must be considered while defining an effective cloud strategy

- **End to end execution framework-** The framework should cater to end-to-end risk management related to a cloud contingency scenario. Further, the framework should be cohesive yet provide sufficient freedom for business owners to make informed decisions.
- **Risks defined with a cloud contingency lens** – New risk categories are defined, or existing categories updated with a cloud contingency lens. Cloud contingency lens focusses on a particular aspect of risks, i.e., a risk that may have an impact on the services of a CSP leveraged by the organization.
- **Alignment with organizational operating model** - Well-defined central/federated ownership for identifying, assessing, monitoring, and addressing risk. The framework should be able to embed according to the organization's operating model with a transparent ownership model.
- **Data-Driven Triaging process** – A data-driven triaging process with a well-defined RACI for all concerned stakeholders at the right level.
- **Exit readiness** – An organization needs to prepare for a planned exit and define a high-level exit plan with a multi-dimensional focus on business, IT, tools, resources, procurement, financial health, etc.

The recommendations listed above can help successfully develop a cloud contingency strategy to cater to a well-planned exit scenario from a CSP.

CONCLUSION

Defining a public cloud exit strategy is a must for any organization that leverages the services of a public cloud irrespective of the cloud maturity level or hosting type.

In addition, the organizations need to effectively and continually monitor and respond to a comprehensive set of risks associated with a cloud service provider.

And therefore, a Cloud Contingency Framework needs to be an integral part of any organization's broader contingency plan.

References

- https://news.microsoft.com/en-nz/2020/05/06/aotearoa-disclosure/
- https://mesh7.com/why-are-amazon-s3-breaches-on-the-rise-and-what-can-we-do-about-it/
- https://redmondmag.com/blogs/scott-bekker/2020/07/sophos-public-cloud-security.aspx
- https://www.securitymagazine.com/articles/96098-critical-azure-security-vulnerabilities-affects-large-organizations
- https://www.forbes.com/sites/saibala/2021/06/22/amazon-continues-its-bold-expansion-into-healthcare-as-aws-launches-a-new-healthcare-accelerator/?sh=69114c17b41d
- https://www.insurancebusinessmag.com/us/news/technology/amazon-dips-its-toes-into-insurance-with-new-partnership-249646.aspx
- https://www.intechopen.com/chapters/74885
- https://www.nytimes.com/2017/06/16/business/dealbook/amazon-whole-foods.html

MEET THE EXPERTS

SHAN YONG
Partner, Head of CIO Advisory APAC
Shan.Yong@infosysconsulting.com

MEGHNA SHEKHAR
Associate Partner
meghna.shekhar@infosysconsulting.com

SACHIN MAHAJAN
Principal Consultant
sachin.mahajan02@infosysconsulting.com

consulting@Infosys.com
InfosysConsultingInsights.com

LinkedIn: /company/infosysconsulting
Twitter: @infosysconsltng

About Infosys Consulting

Infosys Consulting is a global management consulting firm helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage. To see our ideas in action, or to join a new type of consulting firm, visit us at www.InfosysConsultingInsights.com.

For more information, contact consulting@infosys.com