CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Cloud Reassurance: A Framework to Enhance Resilience and Trust

John Pendleton, Ariel (Eli) Levite, and Bob Kolasky

Information and services moved to the cloud offer agility and higher basic security, allowing users to outsource their information technology needs. Consumers increasingly rely on cloud service providers to store and process their information (including critical mission elements) as well as the software to support their work. Over time, cloud services have become concentrated, with around two-thirds of global cloud services managed by three "hyperscale" providers.

Such a high concentration for cloud services is dramatically and irreversibly altering the way IT services are delivered. The rapid emergence of artificial intelligence (AI) further spotlights the potential risks accompanying this transition. The large language models being developed require massive computer resources, which are provided by cloud services. As society and commerce become even more reliant on an AI-enmeshed cloud, the resilience of that cloud will be crucial.

This paper explores the challenges and benefits associated with this level of dependence and concentration of cloud services, the various risks that can result, and desirable actions to minimize and manage those risks. The assessment focuses on resilience—the ability to anticipate and prepare for systemic hazards of all sources, reduce their impact, and recover from them.

Private-Sector Recommendations

Private-sector organizations should utilize the proposed *Cloud Resilience Framework* to build and expand existing efforts with an eye toward greatly enhancing resilience of the cloud as well as the customers in the cloud. Resilience requires incorporating more stakeholders—including insurers, critical infrastructure providers (such as energy) to cloud services, and government policymakers. The four-part framework summarized below lays out foundational policy commitments and suggests actions that would enhance both resilience and trust in the cloud system.

Framework Area	
Foundational commitments	Public commitments to advance cloud-related security and resilience and minimize digital harms.
Resilience of the cloud system	Actions that cloud providers can take to demonstrate and increase resilience of their cloud services.
Resilience of customers	Working with customers, insurers, and other stakeholders to develop a standards-based Resilience Maturity Model.
Exercises and stress tests	Scenario-based exercise programs to validate contingency plans and test capabilities as well as identify best practices and lessons learned.

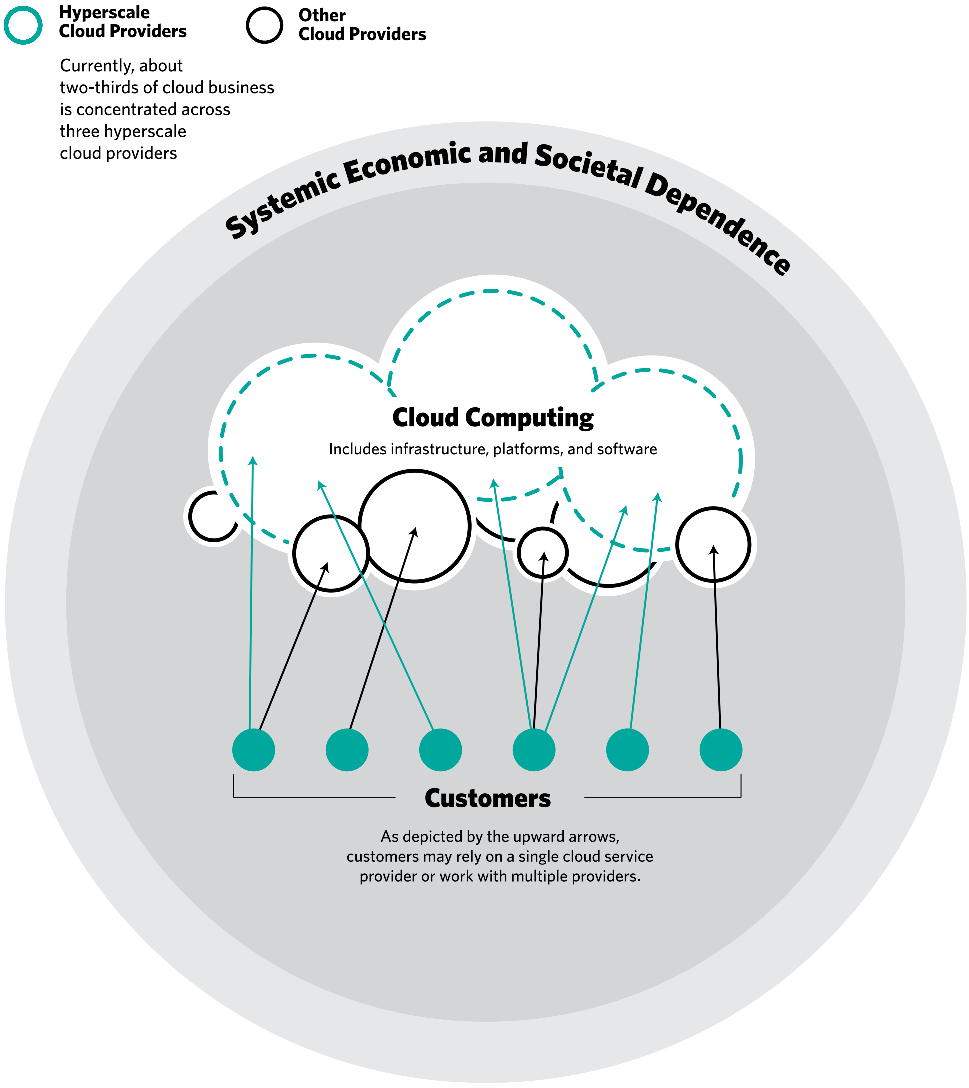
"Cloud Reassurance: A Framework To Enhance Resilience And Trust," is available at CarnegieEndowment.org

Policy Recommendations

Policymakers should enable and support the proposed Cloud Resilience Framework, which should inform and complement ongoing regulatory considerations. Continuing to collaborate with industry will be crucial. Cloud services are a shared benefit to societies, and their availability and resilience needs to be recognized as a shared goal. Among other actions, the path forward should:

- emphasize the cross-sectoral criticality of cloud services;
- ensure improved transparency of risk information;
- expand exercise programs and stress testing; and
- support the development of a functioning re/insurance market to manage cyber-related risks, including those that arise from cloud dependency.

Growing Economic and Societal Dependence on Hyperscale Cloud Services Providers


Hyperscale Cloud Providers
Other Cloud Providers
Systemic Economic and Societal Dependence
Cloud Computing
Customers

Currently, about two-thirds of cloud business is concentrated across three hyperscale cloud providers

Includes infrastructure, platforms, and software

As depicted by the upward arrows, customers may rely on a single cloud service provider or work with multiple providers.

Ariel (Eli) Levite is a nonresident senior fellow in the Nuclear Policy Program and Technology and International Affairs Program at the Carnegie Endowment.
Eli.Levite@ceip.org

John H. Pendleton serves as a nonresident scholar in the Technology and International Affairs Program. Prior to joining Carnegie, he served almost thirty-five years at the U.S. Government Accountability Office (GAO).
John.Pendleton@ceip.org

Bob Kolasky is a nonresident scholar in the Technology and International Affairs Program and is senior vice president for critical infrastructure at Exiger, where he focuses on developing cutting-edge third-party risk management solutions for the critical infrastructure community.
Bob.Kolasky@ceip.org

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.