Others

Below are measures insurers, corporate auditors, utility companies, and other key stakeholders can take to make progress on individual cloud governance issues. Issues for which these stakeholders do not play a clear role have been excluded for concision.

Security & Robustness

Cloud Certification and Auditing

- *International standard setting bodies:* Lay out high-level best practices for increasing the consistency of certification requirements across sectors and functions.

Incident Handling Procedures

- *Insurers:* Consider making reporting requirements a condition for coverage.
- *Insurers:* Collaborate in the development of standards to ensure confidentiality in sharing of sensitive incident information. (Shared with Cloud Providers and Customers.)
- *Insurers and credit rating agencies:* Work with cloud providers, customers, and other key stakeholders to determine appropriate disclosure constituencies, documentation, and timelines.[1] (Shared with Governments, Cloud Providers, and Customers.)

Resilience

Data Retrievability and Back-up Arrangements

- *Insurers:* To encourage widespread and effective use of data retrievability and backup arrangements, insurers may consider requiring data retrievability and backup arrangements as part of their conditions for coverage.
- *Insurers:* Facilitate conversations between governments, customers, and providers on the latter's global dependencies and common mode failures.

Government Intervention in Extremis

- Work with cloud providers or third-party insurers to ensure sensitive data is protected against potential abuse or mismanagement in the event of government intervention. (Shared with cloud providers.)

- *Enterprise customers:* Ensure they are insured against potential abuse or data mismanagement in cases of intervention. (Shared with cloud providers.)
- *Enterprise customers:* Participate in working groups between governments, providers, and enterprise customers to delineate clear "disaster level" thresholds for government takeover and eventual release. (Shared with governments and cloud providers.)
- *Enterprise customers:* Increase cooperation with governments and providers by participating in joint preparedness exercises. (Shared with governments and cloud providers.)

Insurance for Cloud Services

- *Insurers:* May require transparency and reporting measures before agreeing to provide coverage.
- *Insurers:* May partner with cloud[2] as well as to drive mainstream adoption of cyber insurance by customers.[3]
- *Insurers:* Establish standards for transparency on customer's economic burden for insurance products.
- *Insurers:* Help develop a common method for assessing the cost of business interruption arising through cloud events. (Shared with Cloud Providers and Enterprise Customers.)
- *Insurers:* Establish multi-stakeholder dialogues (involving (re)insurers, government, providers, and so on) to increase transparency and understanding around responsibility and accountability in the event of backstopping.
- *Insurers:* Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with Governments, Cloud Providers, and Enterprise Customers.)

Portability and Interoperability

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

Prosperity & Sustainability

Environmental, Community, and Energy Market Impact

- *Utility companies:* Collaborate with cloud providers to identify "brownfield" sites[4] for constructing dedicated utility-scale electricity generation projects. (Shared with cloud providers.)

Human & Civil Rights

Cloud Access Restrictions and Content Moderation

- *Independent, third-party corporate auditors:* Carry out algorithmic audits of cloud providers' and their customers' content moderation technologies.

Ensuring a Beneficial and Safe Digital Environment for Groups with Special Requirements

- *International organizations:* Spearhead or expand current initiatives that ensure a safe and beneficial digital environment for vulnerable groups.[5]

Privacy Protections

- *Civil rights and other nongovernmental public interest groups:* Consult relevant parties (for example, privacy professionals and consumer groups) to craft policies that ensure user privacy and vital information is protected. Then, provide government or corporations with these recommendations.
- *Civil rights and other nongovernmental public interest groups:* Provide victims of privacy intrusion with legal counsel, represent them in cases of legal dispute.

Notes

[1] See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, 26 October 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.

[2] For example, enabling insurers to connect data to the underwriting process, streamlining applications, and facilitating the continuous monitoring of enterprise insurance customers' security posture over time. See: Larry Dignan, "Google Cloud, Allianz, Munich Re team up on cyber insurance program," ZDNet, March 2, 2021, https://www.zdnet.com/article/google-cloud-allianz-munich-re-team-up-on-cyber-insurance-program/.

[3] With Accenture arguing that online service providers such as Google and Amazon may be better suited to respond the increasing "switching risk" by insurance customers, as technology providers are better positioned to develop more personalized services and innovate in pricing strategies (with 35 percent of respondents to their survey expressing that they would be comfortable with insurance providers accessing their behavioral information in exchange for reduced policy costs). See: Erik J. Sandquist, "Prospering in the switching economy," Accenture, n.d., https://insuranceblog.accenture.com/prospering-in-the-switching-economy.

[4] "Brownfield" refers to sites that are often difficult to use for other purposes due to contamination, the presence of hazardous substances (for example, former gas stations and landfills). Development of these sites often requires significant investments in pre-development cleanup, revitalization, and monitoring to remain in compliance with local laws. Cloud providers are well-positioned, due to their size and affluence, to overcome these hurdles, reducing the development pressure on "greenfield" sites, undeveloped land that may be used for agricultural purposes. See: EPA, "Overview of EPA's Brownfields Program," United States

Environmental Protection Agency, https://www.epa.gov/brownfields/overview-epas-brownfields-program.

[5] "What we do," UNICEF, n.d., https://www.unicef.org/what-we-do.