Customers

Below are measures customers* can take to make progress on individual cloud governance issues.

Security & Robustness

Cloud Certification and Auditing

- Work with governments and cloud providers and customers to define high-level performance-based requirements and metrics for confidentiality, integrity, and availability of cloud services. These can differ based on the types of cloud service offered (such as storage and virtualization) and sectoral criticality. (Shared with governments and cloud providers.)

Incident Handling Procedures

- Proactively identify and define in contracts and/or SLAs roles in incident response and crisis communication vis a vis different cloud incident scenarios.[1] (Shared with cloud providers.)
- Collaborate in the development of standards to ensure confidentiality in sharing of sensitive incident information. (Shared with cloud providers and insurers.)
- Work with cloud providers, customers, insurers, credit rating agencies and pertinent regulators to determine appropriate disclosure constituencies, formats, and timing.[2] (Shared with governments, cloud providers, and insurers.)
- *Enterprise customers:* Understand and identify their critical functions and dependencies in order to inform adoption of a risk-based approach.
- *Enterprise customers:* Participate in incident response simulation exercises. (Shared with governments and cloud providers.)

Localization and Routing Requirements

- *Enterprise Customers:* Wish to retain the ability to move and keep data where they want it secure.[3]
- Seek robust protections against unauthorized access and invasion of privacy, which may occur through localization and routing requirements.
- Commit to and encourage the adoption of actions that enhance routing security.[5]

Security and Privacy in Lawful Government Access

- *Enterprise customers:* Publish, on a regular basis, transparency reports detailing aggregate statistics on government access requests (including requests received from foreign governments).[4] (Shared with cloud providers.)
- *Enterprise customers:* Develop industry standards for challenging certain overbroad government access requests (such as requesting unfettered access, encryption keys, ability to break encryption). (Shared with cloud providers.)

Resilience

Data Retrievability and Back-up Arrangements

- *Enterprise customers:* Configure a disaster recovery strategy for each application and service.[5]
- *Enterprise customers:* Regularly carry out drills to test disaster recovery plans.[6] (Shared with cloud providers.)
- *Enterprise customers:* Consider alternatives to their primary cloud provider when procuring backup services, and consider the routine use of at least one additional cloud provider for regular operations.
- *Enterprise customers:* In addition to cloud-based backups, consider enabling on-premises backups for the most critical workloads.
- *Enterprise customers:* Consider incorporating disaster and data recovery strategies into contractual requirements (facilitated by industry's development of guidance materials).
- *Enterprise customers:* Consider adopting practices compliant with international and other key information security standards (such as SOC 2[7] and ISO27001[8]). (Shared with cloud providers.)

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

- *Enterprise customers:* Engage in efforts to map their evolving cloud dependency risks and collaborate with insurers to develop cloud insurance. (Shared with Insurers.)
- *Enterprise customers:* Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with governments, cloud providers, and insurers.)

Portability and Interoperability

- *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.[9]
- *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 governments and providers. Definitions for these terms have been formalized in standards, including SWIPO's Codes of Conduct,[10] IEEE's P2301/P2302,[11] and ISO/IEC's 19941.[12]

Consumer & Enterprise Protection

Commercialization of Customer Data

- Insist on fair and transparent arrangements on use of consumer/enterprise-derived data hosted on the cloud by cloud providers.
- *Industry associations:* Develop and publish model contracts that expand customer choice and bargaining power and restrict the purposes for which customer data may be used by providers.

Prosperity & Sustainability

Environmental, Community, and Energy Market Impact

- Support cross-sector and -industry initiatives to reduce carbon emissions and harmful waste through the development of guidance materials and communication of best practices.
- Adopt use of more sustainable server cooling methods.[17]
- Commit to reduce and improve water usage in data centers.[18]
- Providers may need to also focus on carbon capture/removal strategies.
- Collaborate with utility companies to identify "brownfield" sites[19] for constructing dedicated utility-scale electricity generation projects. (Shared with governments and utility companies.)

- Support the construction of healthier and sustainable buildings (that is, buildings that utilize materials that are safe for humans and the environment, as well as easier to recycle) and possibly leverage existing resources.[20]
- Understand and mitigate the adverse impact of cloud infrastructure creation and operation on local communities. (Shared with governments.)
- Leverage existing carbon emission reduction initiatives (for example, the Climate Neutral Data Centre Pact[21] and the Transform to Net Zero Initiative[22]).
- Commit to regular public reporting on key sustainability indicators, including energy and water consumption and progress toward sustainability targets.
- Whenever possible, encourage supply chain vendors to adopt similar sustainability principles/best practices.
- Share information and lessons learned on building a more sustainable cloud computing business and physical infrastructure.[23]
- Create consultation requirements with local communities and evaluate existing adjudication mechanisms. (Shared with governments.)
- Encourage the transition to a more sustainable business through the use of internal carbon pricing.[24]
- Integrate carbon reduction requirements into procurement policies.[25]

Human & Civil Rights

Cloud Access Restrictions and Content Moderation

- Familiarize themselves with their data rights and protections against bias.
- Notify relevant public entities when suspected instances of bias in content moderation do occur.
- *Consumer Customers:* Use redress mechanisms made available by providers and government.
- *Enterprise Customers:* Solicit public feedback before adopting/updating content moderation policies, practices, and technologies.
- *Enterprise Customers:* Create internal review boards responsible for reviewing content moderation decisions.[13]
- *Enterprise Customers:* Ensure affected parties can challenge content removal, that the ability to do so is clear, and the procedure thereof is straightforward.
- Where possible and effective, use bargaining power (for example, threatening to move or stop using platforms or providers) to compel providers to be more transparent and accountable.
- Establish customer networks to facilitate discourse and disseminate information regarding changes in governmental and/or corporate policy and practices.

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

- *Enterprise customers:* Establish clear policies that ensure enterprise operations do not (whether directly or indirectly) cause or facilitate harm or exploitation of vulnerable groups.
- *Enterprise customers:* Build technical protections for vulnerable groups into platforms (such as limits on recommendation algorithms, and special readable text for the differently-abled).[14] (Shared with cloud providers.)
- *Consumer customers:* Ensure that children are engaging in safe digital environments by monitoring and appropriately curating content, using privacy controls and other restrictions, researching platforms, and so on.

Privacy Protections

- Adopt basic measures that prevent/discourage cyber intrusions (for example, frequently changing passwords, two-factor authentication limiting what information is made public or shared with providers, and so on).
- *Enterprise Customers:* Work with cloud service providers to ensure user identity and information are protected.
- *Enterprise Customers:* Provide clear language on the allocation of responsibility between providers and customers for data privacy. (Shared with Providers.)

Notes

* In this project, "customer" always refers to both enterprises and individual consumers, who use "enterprise cloud" and "consumer cloud" deployments, respectively. Where necessary, individual bullets are labeled with "Enterprise Customers" or "Consumer Customers" to specify that a certain interest, action, or concern is held only by one of these two types of customers.

[1] Cloud providers and their customers should develop and integrate incident notification matrices in their SLAs and/or contracts, laying out each party's responsibilities in crisis communications. For instance, the Cloud Security Alliance sets out the following division of responsibilities for various cloud incident response scenarios: (1) For a security incident occurring in the platform or service layer for a PaaS or SaaS application, the response should be driven by the cloud provider; (2) if a security incident is occurring in the application layer for a PaaS application, the customer should be driving the response; and (3) in the case of a security incident occurring in the platform layer for an IaaS infrastructure cloud, the response should be driven jointly by the customer and the cloud provider to determine if it originated in the customer's environment or the cloud provider's environment. (See: CSA, "Cloud Incident Response (CIR) Framework," Cloud Security Alliance (CSA), 4 May 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.) Additionally, the retention of digital forensic evidence should be seen as a shared responsibility. (See: Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," *ScienceDirect, Digital Investigation*, vol. 9, issue 2, November 2012, pages 71-80, https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X.)

[2] 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/.

[3] The localization of data in-territory does not guarantee its security. Data security is attained through encryption and robust zero-trust system architectures.

[4] Many enterprise customers already produce information request reports on a voluntary basis, as part of their corporate social responsibility commitments. See: Twitter, "Information Requests," Twitter Transparency Center, 2021, https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec.

[5] 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.

[6] Providers may issue guidance to help customers simulate disaster scenarios to test their recovery strategies against. For instance, see: Microsoft, "Performing disaster recovery drills," Microsoft Azure, October 18, 2021, https://docs.microsoft.com/en-us/azure/azure-sql/database/disaster-recovery-drills; and Google, "Disaster recovery scenarios for data," Google Cloud, n.d., https://cloud.google.com/architecture/dr-scenarios-for-data.

[7] AICPA, "SOC 2 – SOC for Service Organizations: Trust Services Criteria," AICPA, n.d., https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.

[8] ISO, "ISO/IEC 27001: Information Security Management," ISO, n.d., https://www.iso.org/isoiec-27001-information-security.html.

[9] 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/.

[10] "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/.

[11] 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/.

[12] "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.

[13] See, for example, Facebook's Oversight Board, "Oversight Board Home Page," Oversight Board, n.d., https://oversightboard.com/.

[14] Sarah Perez, "TikTok to add more privacy protections for teenaged users, limit push notifications," TechCrunch, August 12, 2021, https://techcrunch.com/2021/08/12/tiktok-to-add-more-privacy-protections-for-teenaged-users-limit-push-notifications/.