Cloud Certification and Auditing

As they move increasingly critical workloads onto the cloud, both governments and enterprise cloud customers seek high levels of trust in the security and availability of their cloud services. Certification programs seek to address these demands by requiring cloud providers or individual cloud services to meet certain technical and assurance criteria. Certifications can differ dramatically in scope and sector. Some, like FedRAMP,[1] are designed to ensure the security of cloud services used across the U.S. federal government. Others are more narrowly tailored to provide assurance for especially critical or sensitive functions in key sectors. Certification programs can also be used to increase customer confidence in the nonsecurity qualities of cloud services, such as their environmental impact. However, certifications are not a panacea, and many stakeholders see existing certifications as insufficient to address their concerns about the security and robustness of cloud services. This section explores the key challenges associated with designing, improving, and implementing cloud certification programs.

Key Considerations

- ***Overfocused on cybersecurity.*** Certification programs are regularly designed to increase customer confidence in the cybersecurity of cloud systems, but often neglect to account for the threats posed by nonmalicious triggers of failure, such as natural disasters, human error, and technical malfunctions. This may lead regulators and customers to be overconfident in the security and robustness of cloud systems and take for granted cloud providers' efforts to address these concerns on their own.
- ***Impact on agile tech development***. Certification schemes may be resource- and time-intensive for the entities processing the certification as well as for the providers undergoing the assessment, as they require both initial as well as continuous monitoring processes, coordination between government representatives or other third-party auditors, subject-matter and technical expertise, and so on.[2] These requirements and processes also risk delaying the delivery of new products and services, as these must also undergo certification.
- ***Limited government capabilities.*** Governments struggle to audit cloud services and operations because such auditing is resource-intensive. Moreover, the rapid pace of innovation in cloud services makes it challenging for the government to keep up, since the greatest expertise lies with those involved in developing and operating the technology.
- ***Regulatory redundancies and inconsistencies***. Harmonizing certification requirements is essential to prevent regulatory redundancies, inconsistencies, and fragmentation across regions and sectors. Moreover, though there is a desire to be able to use existing certifications as evidence of reliable security practices when seeking certifications in other

sectors or jurisdictions, the requirements in one sector's program may not map onto those of another. Greater consistency across jurisdictions and functions would reduce regulatory compliance burdens for cloud providers and customers.

- ***Unclear roles and responsibilities***. Roles and responsibilities may be unclearly or inconsistently divided between auditing entities (for example, government agency representatives and third-party or corporate auditors). This may lead to inconsistencies in the way providers are assessed for compliance with certification requirements.

Stakeholder Perspectives

Government

- Are struggling to find ways to enhance surety of the cloud services on which critical sectors, such as finance, depend.
- Seek a greater role in developing certifications for public cloud services.

Cloud Providers

- Have a general interest in assurance programs and processes that are consistent with agile tech and business development, are universally applied across providers, avoid redundancy, and are risk-based and outcome-focused.

Customers

- Welcome arrangements, such as certification programs, that enable them to understand cloud risks and assess providers' security and robustness in order to ensure the protection of privacy and continuation of service under duress.[3]
- *Enterprise Customers:* Seek to leverage cloud certifications to meet their own compliance and transparency requirements.

Others

- N/A

Tensions with Other Cloud Governance Issues

- ***Effects of Cloud Market Concentration:*** Stringent security requirements and the associated compliance costs could increase barriers to market entry for nascent providers.
- ***Environmental, Community, and Energy Market Impact:*** While certification programs can be used to drive progress on nonsecurity issues, such as the environmental sustainability of

cloud services, such programs may raise similar challenges as security-focused programs. Moreover, certain elements of a security or robustness-focused certification program, such as maintaining redundant infrastructure in order to guard against the possibility of natural disaster-induced outages, could conflict with sustainability goals, which generally involve minimizing the physical presence and carbon footprint of the cloud.

Potential Ways Ahead

Government

- Improve communications channels between government and industry to provide feedback on and refine existing certifications processes by identifying areas in need of adjustment. These include a clear delineation of roles and responsibilities among auditing entities, irregularities in risk assessment, and validation across authorizers. (Shared with Cloud Providers.)
- Work with cloud providers and enterprise 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, virtualization, and so on) and sectoral criticality.

Providers

- Improve communications channels between government and industry to provide feedback on and refine existing certifications processes by identifying areas in need of adjustment. These include a clear delineation of roles and responsibilities among auditing entities, irregularities in risk assessment, and validation across authorizers. (Shared with Governments.)
- Work with governments and enterprise customers to define high-level performance-

Customers

- 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, virtualization, and so on) and sectoral criticality. (Shared with Governments and Cloud Providers.)

Others

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

(Shared with Providers and Enterprise Customers.)
- Distinguish between requirements for less and more sensitive government workloads and align certification criteria with those requirements.
- Make audits of performance/compliance public or mandate provider's transparency on 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, virtualization, and so on) and sectoral criticality. (Shared with Governments and Enterprise Customers.)
- Help customers understand their new or potentially modified responsibilities under future performance-based certifications.

Recent Examples and Additional Resources

- "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *The New York Times*, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html
- "The CLOUD Act is an important step forward, but now more steps need to follow," Microsoft (Blog), April 3, 2018, https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/
- "The need for a Digital Geneva Convention," Microsoft (Blog), February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.
- "The Cybersecurity 202: Paul Manafort's case may undermine the FBI's encryption argument," *The Washington Post*, June 6, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-

202/2018/06/06/the-cybersecurity-202-paul-manafort-s-case-may-undermine-the-fbi-s-encryption-argument/5b16ae5e1b326b08e8839150/?no_nav=true.
- "Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy," OECD, December 2020, https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm.
- "WhatsApp adds end-to-end encryption to chat backups, locking up data in the cloud," Cyber Scoop, September 10, 2021, https://www.cyberscoop.com/whatsapp-encryption-backup-chats/.

Notes

[1] See: Microsoft, "Law Enforcement Requests Report." Microsoft, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[2] See: Ju (Lindsay) Zhu, "China Passes New Data Privacy and Security Laws," *The National Law Review*, August 23, 2021, https://www.natlawreview.com/article/china-passes-new-data-privacy-and-security-laws.

[3] In the case of enterprise cloud deployments, cloud providers may re-direct access requests to the owners of the data, the enterprise customers themselves.

[4] A similar effect has been observed in the past. For example, Edward Snowden's revealing of U.S. National Security Agency surveillance programs damaged customer trust in U.S. technology companies and their products, both domestically and globally. See: The New York Times, "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*, March 21, 2014, https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[5] Mechanisms for data storage and backup in the cloud further enhance the appeal of gaining access to the cloud as a repository of data, bypassing restrictions and difficulties of accessing data elsewhere. Trusted Cloud Principles, "Principles." Trusted Cloud Principles, 2021, https://trustedcloudprinciples.com/principles/.

[6] See: Microsoft, "About our practices and your data: Q: Does Microsoft notify its enterprise customers when law enforcement or another governmental entity requests their data?" Microsoft (Blog), n.d., https://blogs.microsoft.com/datalaw/our-practices/#does-microsoft-notify-enterprise-customers.

[7] See: Microsoft, "Law Enforcement Requests Report," Microsoft, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[8] Even when gag orders are not in place, providers may still fail to disclose government access requests to their customers.

[9] See: "Open Letter to GCHQ," Coalition of civil society organizations, technology companies, trade associations, and security and policy experts, May 22, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.

[10] Customers in any given jurisdiction are also citizens/residents and thus have an interest in refraining from utilizing cloud services/providers which undermine or excessively impede government access, to the point where traditional security threats and other undesirable law enforcement outcomes (such as the proliferation of terrorism-related material or CSAM) abounds.

[11] See: Jay Greene and Drew Harwell, "When the FBI seizes your messages from Big Tech, you may not know it for years," *The Washington Post*, September 25, 2021, https://www.washingtonpost.com/technology/2021/09/25/tech-subpoena-secrecy-fight/.

[12] See: U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," U.S. Department of Justice, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download.

[13] See: Trusted Cloud Principles, "Principles," Trusted Cloud Principles, 2021, https://trustedcloudprinciples.com/principles/.

[14] Many cloud providers already produce information request reports on a voluntary basis, as part of their corporate social responsibility commitments. See: IBM, "IBM 1H 2021 Law Enforcement Requests Transparency Report," IBM, 2021, https://www.ibm.com/downloads/cas/DAGAKDJG and Microsoft, "Law Enforcement Requests Report," Microsoft, 2021, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[15] 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.