# The IBM Policy Lab's 10 Recommendations for Stronger Cloud Security Policies

**Mason Molesky**
Cloud Policy & Cybersecurity Policy Executive, IBM

**Howard Boville**
Senior Vice President & Head of IBM Cloud Platform

Industries, from banking and telecommunications to retail and logistics, are faced with cybersecurity concerns as they adopt cloud technology to modernize their core business functions. Our world today depends on the reliable use of cloud technologies – from the cars we drive, to the devices we use, to the purchases we make. As organizations modernize and transition more of their infrastructure management to third-party providers to reap the benefits such as cost sharing, scalability, flexibility, reliability, and enhanced security, one of the biggest risks is an environment of disconnected parts that is difficult to navigate and can be nearly impossible to secure. Strong cloud security policies as outlined below can help companies, especially in regulated industries, address these third- and fourth-party risks and blind spots that bad actors attack.

IBM employs hybrid cloud – the use of both on- and off-premises data centers – to help our clients integrate the best features and functions from any cloud, or traditional IT environment, and achieve connected security systems while automating time-consuming investigative tasks and staying ahead of threats. But it’s not just IBM – many businesses are coming together to prioritize cloud security. As we rely more on the cloud, ensuring security and trust in these systems becomes ever more important. To that end, the IBM Policy Lab puts forth to governments worldwide 10 recommendations for stronger cloud security certification policies.

IBM supports policies that enable governments and industry to use trusted, state-of-the art solutions such as cloud, while not applying overly broad regulations which would hamper continuous innovation and improvements in technology. We also support laws that make concrete improvements to cloud security, such as policies that promote globally-recognized, principle-focused, and technology-neutral cloud security frameworks.

As governments worldwide are establishing certification regimes to provide a level of security assurance for public sector clouds under their purview – including the Federal Risk and Authorization Management Program (FedRAMP) in the United States, the Cybersecurity Certification Scheme for Cloud Services (EUCS) in the European Union, the Information System Security Management and Assessment Program (ISMAP) in Japan  – we offer the following 10 recommendations for sound cloud security certification policies.

1

**A risk-based approach** grounded in industry best practices and research that addresses distinctions between cyber threats, sensitivity of data, and specific uses cases.

2

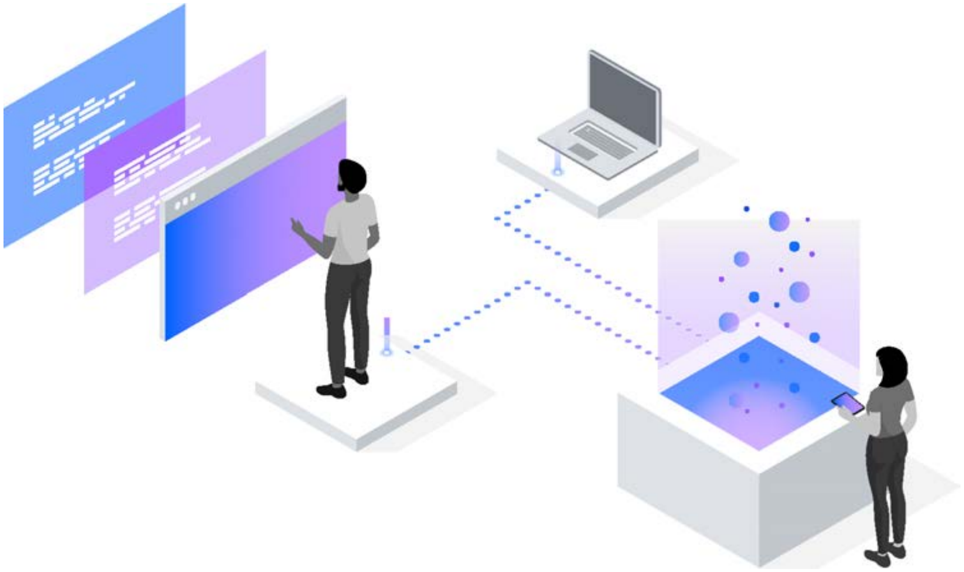
**Flexibility to adopt emerging best practices** so security can evolve more quickly. Policies should be principles-based where standards - such as the U.S. National Institute of Standards and Technology (NIST) Special Publication 53 on Security Controls - can be used to demonstrate these principles without being overly prescriptive or constraining.

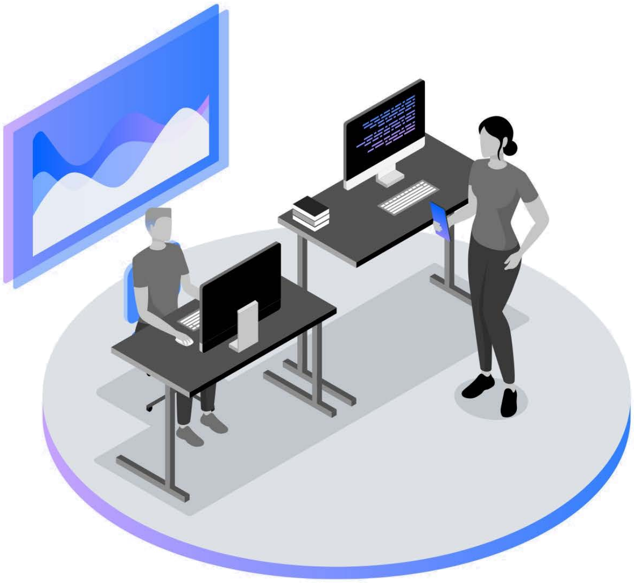
3

**Minimal variation among existing certification regimes** by using recognized standards and global best practices - such as ISO 27001 for information security management systems and ISO 27017 for information security controls - for the provision and use of cloud services.

4

**A shared responsibility model** where responsibility for cybersecurity is shared amongst cloud services providers, clients, and third parties with clearly defined roles and responsibilities.





5 **Client or customer control of their data** and risk-based decisions made by clients or customers on where, how, and when their data is in use, storage, and transmission. Data localization decisions should be made by clients or customers based on risk, data type, and business needs and not required by default as part of a cloud security certification.

6 **Technical mechanisms to build trust**, rather than political or other inconsistent requirements - such as company ownership - which does not guarantee greater cloud security. Instead, technical mechanisms such as Zero Trust Architecture should be used.

7 **Efficient accountability processes** that leverage pooled audits and self-attestations to avoid expensive, slow, and static audit processes.

8 **Consistent security requirements across the digital supply chain** which ensures third, fourth, and other parties – which operate on or provide support services to the cloud – also comply. Companies that consume cloud technologies should ensure through attestation and evaluation these parties also meet the same minimum security standards.

9 **Strong encryption standards that ensure the protection of data** is based on risk, including quantum resistant encryption - like NIST's post quantum cryptography algorithms - and confidential computing, such as hardware-based trusted execution environments which can better protect data while in use.

10 **Automation of the certification process,** where possible, to minimize impact on businesses and speed up the certification process.

IBM is working with industries of all sizes and tailoring sector specific solutions as needed. For example, in 2020 we helped form a Financial Services Cloud Council with executives from over 120 global and regional banking institutions to discuss cloud computing with a focus on de-risking the financial services industry. IBM also created the IBM Cloud Framework for Financial Services, a comprehensive set of control requirements designed to help address the global security requirements and regulatory compliance obligations of financial institutions and cloud best practices. We also have globally-recognized security tools such as IBM's Cloud Security and Compliance Center, which provides centralized management tools, always-on compliance, and up-to-date secure configurations and visibility.

Beyond financial services, we see how effective these tools can be when used, continuously and holistically, to improve security and ensure compliance. Yet, the solutions only work if organizations actually use them. Cybersecurity is a team sport, and we continue to engage and collaborate with various stakeholders and communities worldwide to build trust in these security regimes. Our participation in groups such as Charter of Trust, the Cloud Service Provider Advisory Board, and the Cloud Security Alliance demonstrates our commitment to building cloud security policies that enable trust throughout our customers, users, and partners.

Ensuring the security of cloud technologies will be ever more important as organizations globally look to adopt cloud to power digital organizational transformation and enable the execution of mission. We hope that governments globally will consider these recommendations as they look to develop cloud security certification policies and ensure the full benefits of cloud can be reaped.

IBM Corporation
New Orchard Road
Armonk, NY 10504

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.