ASIA SOCIETY
POLICY
INSTITUTE

Establishing a Positive Regulatory Environment for Cloud Security in APEC

1. Introduction

Cloud computing is a cornerstone of digital transformation across APEC economies, driving economic growth, business efficiency, and innovation. The region's cloud market is expanding rapidly, but cloud adoption varies widely, from under 30% in Indonesia, the Philippines, and Viet Nam to over 70% in Australia, Japan, and Singapore. These disparities reflect differences in regulatory approaches, levels of digital readiness, and market development.

Three major regulatory challenges continue to impact cloud adoption across APEC economies:

1. **Regulatory Fragmentation:** Varying domestic standards and bespoke security frameworks (such as those regulating the use of cloud computing in specific sectors) makes compliance more complex, increasing operational costs for governments and companies – especially small and medium-sized enterprises seeking to do business across borders – and slowing cloud adoption.
2. **Data Localization Requirements:** These policies can create unnecessary barriers to cross-border data flows and limit access to secure, globally competitive cloud solutions.
3. **Inconsistent Cybersecurity Standards:** Divergent regulations raise costs for cloud providers without necessarily improving security outcomes.

The Recommendations for Cloud Transformation in APEC, endorsed in 2023, marked a useful step forward in promoting cloud adoption and aligning regulatory approaches across the region. These recommendations aim to accelerate regional cloud adoption by strengthening digital infrastructure, fostering a supportive regulatory environment, and encouraging the use of risk-based international standards.

This issue brief examines how APEC economies can develop regulatory frameworks that enhance cloud security, build trust, and advance innovation and digital transformation by highlighting successful approaches, the role of international standards, and implementation strategies.

2. Role of International Standards in Strengthening Cloud Security

Regulatory fragmentation presents challenges to data protection, cybersecurity resilience, and securing emerging technologies like AI, particularly as cyber threats operate across jurisdictions. This issue is especially acute for small and medium-sized enterprises, which lack the resources to comply with multiple overlapping regulations. International cybersecurity standards provide a proven framework for addressing these challenges by enhancing trust, improving security, facilitating cross-border data flows, and streamlining compliance requirements.

Key International Standards for Cloud Security

The ISO/IEC 27000 family of standards offers a globally recognized framework for information security management, providing organizations with a systematic approach to securing information assets. Among these, ISO/IEC 27001 is the most widely adopted standard, establishing a foundation for managing information security risk, while other standards address areas such as cloud-specific security responsibilities, incident response, and data protection (see Appendix).

Complementing the ISO standards, other widely recognized frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and NIST SP 800-53, also reflect best practices for cloud security. In addition, the Advanced Encryption Standard serves as the globally recognized benchmark for data encryption; domestic encryption requirements that diverge from this standard often create unnecessary technical barriers.

Cloud security cannot be managed in isolation. As cyber threats evolve, alignment with international standards will be critical for ensuring security while expanding economic opportunities for APEC economies. Adoption of international standards also paves the way for regulators to streamline their requirements and consider granting regulatory reciprocity across jurisdictions.

3. Good Regulatory Practices in Cloud Security

Ensuring predictability and trust in cloud security regulation requires a consistent risk-based approach across economies. The 2023 APEC Good Regulatory Practices Blueprint provides key principles that economies can apply to cloud security policies:

- **Transparency:** Cloud security regulations should be clearly defined, publicly available, and easily accessible to industry stakeholders. Open rulemaking enhances trust and compliance.
- **Public Consultation:** Engaging businesses, civil society, and technical experts in regulatory development can help ensure practical, effective policies.
- **Evidence-Based Policy Development:** Cloud security regulations should be based on risk assessments, international best practices, and regulatory impact analysis to ensure that they are effective and proportionate.
- **Regulatory Coordination:** Aligning cloud security frameworks across agencies and economies can reduce overlapping requirements and trade disruptions.

An adaptive regulatory framework for cloud security requires several key components. Risk-based security models should categorize cloud services by data sensitivity and threat level, ensuring appropriate security measures without creating unnecessary compliance burdens. Clear protocols for incident response and reporting enable cloud providers to manage cybersecurity threats effectively and collaborate with regulators. Ongoing public-private collaboration ensures policies remain relevant as threats evolve, while flexible, technology-neutral regulations allow economies to adapt to emerging technologies like AI while maintaining strong security protections.

Lessons from Effective Cloud Security Models

Several APEC economies have implemented internationally aligned regulatory frameworks that successfully balance security with cloud adoption. The following are two notable examples:

- **Singapore's Multi-Tier Cloud Security Standard (MTCS):** Developed through extensive industry consultation, MTCS is an example of a domestic standard that promotes global interoperability. Building on ISO/IEC 27001, it allows cloud providers to certify at different security tiers based on their risk profile. Singapore has published documentation to facilitate cross-certification between MTCS and ISO/IEC 27001, streamlining compliance for businesses.
- **U.S. FedRAMP (Federal Risk and Authorization Management Program):** By categorizing cloud services based on risk levels, this program enables cloud providers to meet U.S. government security requirements through a standardized certification process. Its "Do Once, Use Many" approach streamlines security assessments, reducing compliance burdens by allowing multiple agencies to rely on a single rigorous evaluation. While it is a domestic program, FedRAMP is based on NIST SP 800-53, aligns with widely recognized security principles, and is referenced internationally as a model for cloud security frameworks.

These models demonstrate that transparent, adaptable, and internationally aligned regulatory frameworks can enhance security while promoting cloud adoption. However, the current lack of reciprocity between such domestic frameworks means that cloud providers often need to meet multiple certification requirements across jurisdictions, highlighting the potential benefits of greater regulatory coordination and mutual recognition mechanisms.

4. Best Practices and Implementation Strategies for APEC Economies

Governments play a pivotal role in driving secure cloud transformation by setting security baselines and leading by example in cloud adoption. Public sector cloud adoption should align with international security standards to create a consistent regulatory framework that sets a precedent for private-sector best practices. A cloud-first or cloud-by-default policy for government IT promotes risk-based security frameworks that enhance flexibility while maintaining strong protections. Effective public sector cloud procurement requires a coordinated approach that standardizes security requirements, reduces costs, and streamlines acquisition across multiple agencies.

Domestic security regulations should maintain interoperability with internationally recognized cloud security certifications and, where feasible, recognize these certifications to minimize duplicate compliance requirements for businesses. Supporting voluntary security certification programs based on established international frameworks can encourage cloud adoption by helping businesses demonstrate compliance without excessive costs.

Encouraging industry-led security guidelines that adapt to sector-specific risks and emerging threats will help ensure regulatory frameworks remain effective and flexible. Strengthening public-private collaboration and cross-border threat intelligence sharing will enhance cyber resilience and help regulators adapt to an evolving threat landscape.

Tailoring Approaches for Different Levels of Cloud Security Readiness

APEC economies are at different stages of cloud adoption and cybersecurity development. Implementation strategies should be flexible and adaptable based on each economy's cloud security readiness.

- **Economies building foundational cloud security capabilities** should prioritize workforce training, knowledge sharing, and government-led adoption. By using technical assistance and capacity-building programs, they can develop risk-based regulatory frameworks that are aligned with international standards. These economies can benefit from a phased approach, starting with foundational security controls and gradually incorporating more advanced measures as capacity is developed. Additionally, promoting government cloud adoption can help establish security best practices while supporting adoption by small and medium-sized enterprises through simplified compliance frameworks.

- **Economies with evolving cloud security frameworks** should focus on strengthening cross-border collaboration to improve regional regulatory convergence and alignment with international standards. Implementing risk-based security requirements will help maintain flexibility while ensuring strong protections against cyber threats. Additionally, developing clear regulatory guidelines for cloud service providers and users will enhance compliance while supporting a more transparent and accountable digital ecosystem.
- **Economies with advanced cloud security frameworks** can play a leadership role in regional coordination efforts to promote interoperability and policy alignment. By sharing expertise and resources, they can support capacity-building initiatives across APEC. Additionally, facilitating regional standards harmonization through collaborative efforts can reduce regulatory fragmentation, including with respect to cybersecurity certification and cross-border data flows.

By implementing scalable, cost-effective regulatory approaches, APEC economies can ensure that businesses of all sizes benefit from a secure cloud ecosystem, supporting economic growth, innovation, and cross-border digital trade.

5. Regional Collaboration and the Way Forward

As cloud computing becomes increasingly integral to APEC economies, cross-border cooperation is essential to ensure secure, interoperable, and innovation-friendly regulatory environments. APEC's institutional framework – including the Telecommunications and Information Working Group (TELWG) and the Digital Economy Steering Group (DESG) – provides valuable platforms for facilitating regional regulatory alignment and technical collaboration. However, in light of the growing strategic and economic importance of cloud security, discussions should be elevated beyond technical groups to ensure high-level policy engagement and concrete action. To advance regional cloud security efforts, APEC economies should take the following actions:

- Use the APEC Cloud Recommendations as a call to action for economies to agree that aligning domestic cloud security policies with international standards is best practice.
- Promote the integration of internationally recognized cloud security standards into domestic policies to improve interoperability and enhance cross-border digital trade and services.
- Utilize APEC to facilitate regulatory dialogue to improve transparency, promote alignment with international cybersecurity frameworks, and explore opportunities for mutual recognition of security certifications. As a practical first step, conduct a mapping of cloud security certification requirements across APEC economies to identify common elements and differences, laying the groundwork for greater interoperability.
- Expand APEC-led capacity-building programs to accelerate cloud security adoption in economies at earlier stages of implementation.
- Strengthen public-private partnerships between governments, industry, and technical experts, leveraging groups such as the APEC Business Advisory Council and Asia-Pacific Services Coalition to incorporate business input.

By building on APEC's existing digital economy agenda and aligning with international standards, economies can foster regulatory coherence, enhance cloud security, and position the region as a leader in the global digital economy.

Appendix: Key International Standards for Information Security Management

The **ISO/IEC 27000** family includes several standards relevant to cloud security:

- **ISO/IEC 27001 (Information Security Management System):** Provides a globally recognized framework for managing information security risk.
- **ISO/IEC 27002 (Information Security Controls):** Provides guidelines for information security standards and information security management practices.
- **ISO/IEC 27017 (Cloud Security Controls):** Defines cloud-specific security responsibilities, offering guidelines for both providers and users.
- **ISO/IEC 27018 (Personal Data Protection in the Cloud):** Focuses on protecting personal data in cloud services, aligning with global privacy regulations.
- **ISO/IEC 27035 (Information Security Incident Management):** Provides guidelines for incident management, including how to prepare for, detect, and respond to information security incidents.
- **ISO/IEC 27040 (Security Guidance for Storage Systems and Ecosystems):** Provides guidelines for storage security, addressing specific risks and controls related to data storage.

The Asia Society Policy Institute and the Asia Society take no institutional positions on matters of public policy and other issues addressed in reports and publications they sponsor. All statements of fact and expressions of opinions contained in this report are the sole responsibility of its authors and may not reflect the views of the organization and its board, staff, and supporters.

This issue brief was made possible through the generous support of the Coalition of Services Industries (CSI) and benefited from the valuable insights of the Australian Services Roundtable (ASR).