ITI Promoting Innovation Worldwide

Considerations Around Cybersecurity Certification

Courtney Lang | Senior Director of Policy

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
itic.org

ITI Promoting Innovation Worldwide

ITI Member Companies

ITI's *Policy Principles for Cybersecurity Certification*

- We released a set of policy principles on cybersecurity certification in September 2020.
- These principles are intended to provide guidance to policymakers who are considering implementing certification as a means to improve cybersecurity.
- Offer a foundational understanding of cybersecurity certification, including the limitations of such an approach.

ITI
Promoting Innovation Worldwide

Cybersecurity certification is not a comprehensive solution

- Certification only reviews information about security at a specific point in time and does not necessarily equate to security or reduced risk.
  - ➢ It *cannot* represent a complete picture of security because of the way in which the threat landscape evolves.
- Because threats are dynamic and constantly changing, the long period of time that it takes to complete a certification will in many cases mean that the product/service is no longer at the leading-edge of security by the time the certification is complete.
- Cybersecurity is a shared responsibility between vendors, consumers, and government.

ITI
Promoting Innovation Worldwide

Consider that it may be more appropriate to evaluate an ICT vendor's practices, instead of the end product itself

- How a vendor develops its products and services is often a more appropriate indicator of how secure the end products or services will be than a point-in-time certification.
- Vendor practices to consider range from secure development and testing practices through continual vulnerability assessment, management and mitigation to supply chain risk.

Take a risk-based approach to cybersecurity certification requirements

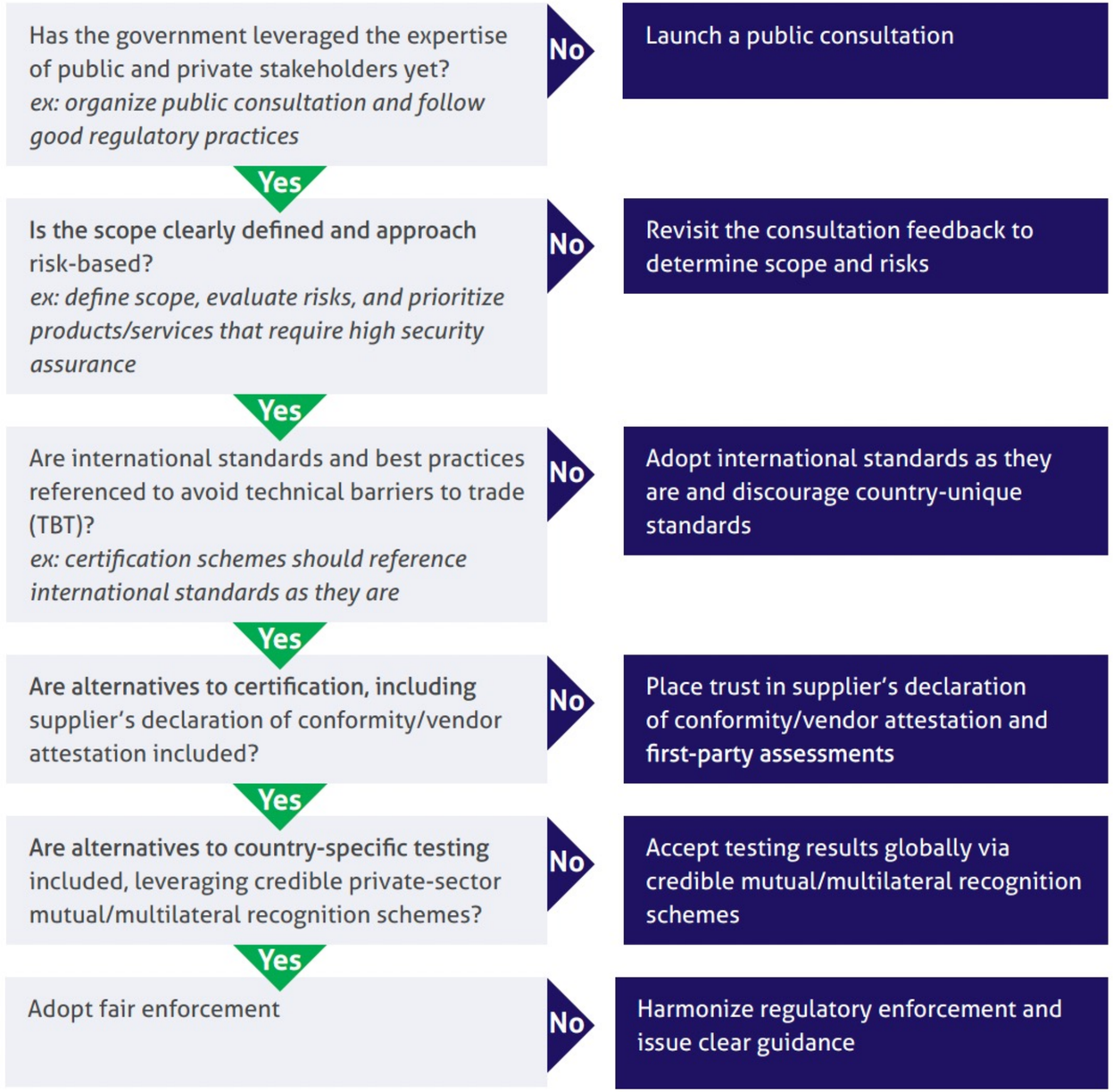
- Any certification scheme should be based on a comprehensive risk assessment so that it is appropriately targeting those products, services, or processes that require high security assurance.
- Certification requirements should not be applied across an entire sector (i.e. telecom equipment sector), as this would be anathema to a risk-based approach.
- We encourage regulators to undertake a threat assessment to understand the landscape and further, seek to determine and identify critical components.
  - i.e.) EU Coordinated Risk Assessment on Cybersecurity of 5G Networks

ITI
Promoting Innovation Worldwide

Reference international standards to avoid erecting technical barriers to trade

- Certification schemes should be grounded in international, industry-led consensus standards and best practices.
- These standards should be adopted as written and published
  - Deviations can negatively impact international trade, requiring suppliers to meet different technical specs in different markets.
- Common process-based cybersecurity controls include ISO/IEC 27000 and IEC 62443.
- Certification schemes should be technology-neutral and refrain from mandating specific technical features or controls.

ITI
Promoting Innovation Worldwide



ITI

Promoting Innovation Worldwide