Policy Principles for Cybersecurity Certification

September 2020

ITI
Promoting Innovation Worldwide

September 2020

Executive Summary

ITI is the global association of the tech industry and our membership comprises over 70 leading technology and innovation companies from all corners of the ICT industry, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies. We recognize that governments around the world are considering mandating cybersecurity certification schemes for products, services, or company processes for the purpose of gaining more confidence in those product/services/companies in their respective markets. ITI respects that governments contemplating mandatory regulations for cybersecurity certification are well intentioned. **However, cybersecurity certification is not a comprehensive, one-size-fits-all solution, nor should it be considered a solution of first resort.**

Policymakers should be aware that certification only reviews information about security at a specific point in time and does not necessarily equate to security or reduced risk. Further, because threats are dynamic and constantly changing, the long period of time and effort required to complete a certification in many cases means that a certified product or service may no longer be at the leading edge of security and may not account for the latest innovations to address ever-evolving cyber threats.

Nonetheless, if governments choose to set regulations to mandate certification schemes even after recognizing the limitations of certification, we recommend they follow six key considerations:

- ✓ **Leverage the Expertise of Public and Private Stakeholders and Ensure Transparency.** Any government certification schemes should be proposed and adopted through an open and transparent process that allows for stakeholder input and public comment.
- ✓ **Take a Risk-based Approach and Clearly Define the Scope of Certification Schemes**. Any certification schemes should be based on appropriate risk factors, with priority given to certification schemes requiring high security assurance.
- ✓ **Reference International Standards and Best Practices as the Technical Basis to Avoid Technical Trade Barriers.** Cybersecurity certification schemes should be grounded in international, industry-driven, voluntary consensus standards and best practices.
- ✓ **Consider Alternatives to Certification such as Supplier Declarations of Conformity or Vendor Attestations.** Alternatives to certification are widely accepted in the marketplace to demonstrate compliance and industry has extensive experience with such mechanisms.
- ✓ **Recognize Supplier/Vendor Assessments, Avoid Localized Testing, and Leverage Mutual Recognition Schemes.** Governments should accept supplier/vendor assessments and recognize competent testing labs owned by suppliers/vendors. If third-party assessments are necessary, localized testing should be avoided and mutual/multilateral recognition schemes leveraged.
- ✓ **Adopt Fair Enforcement.** Ensure harmonized regulatory enforcement and guidance, including appropriate market surveillance, to accelerate industry adoption of schemes.

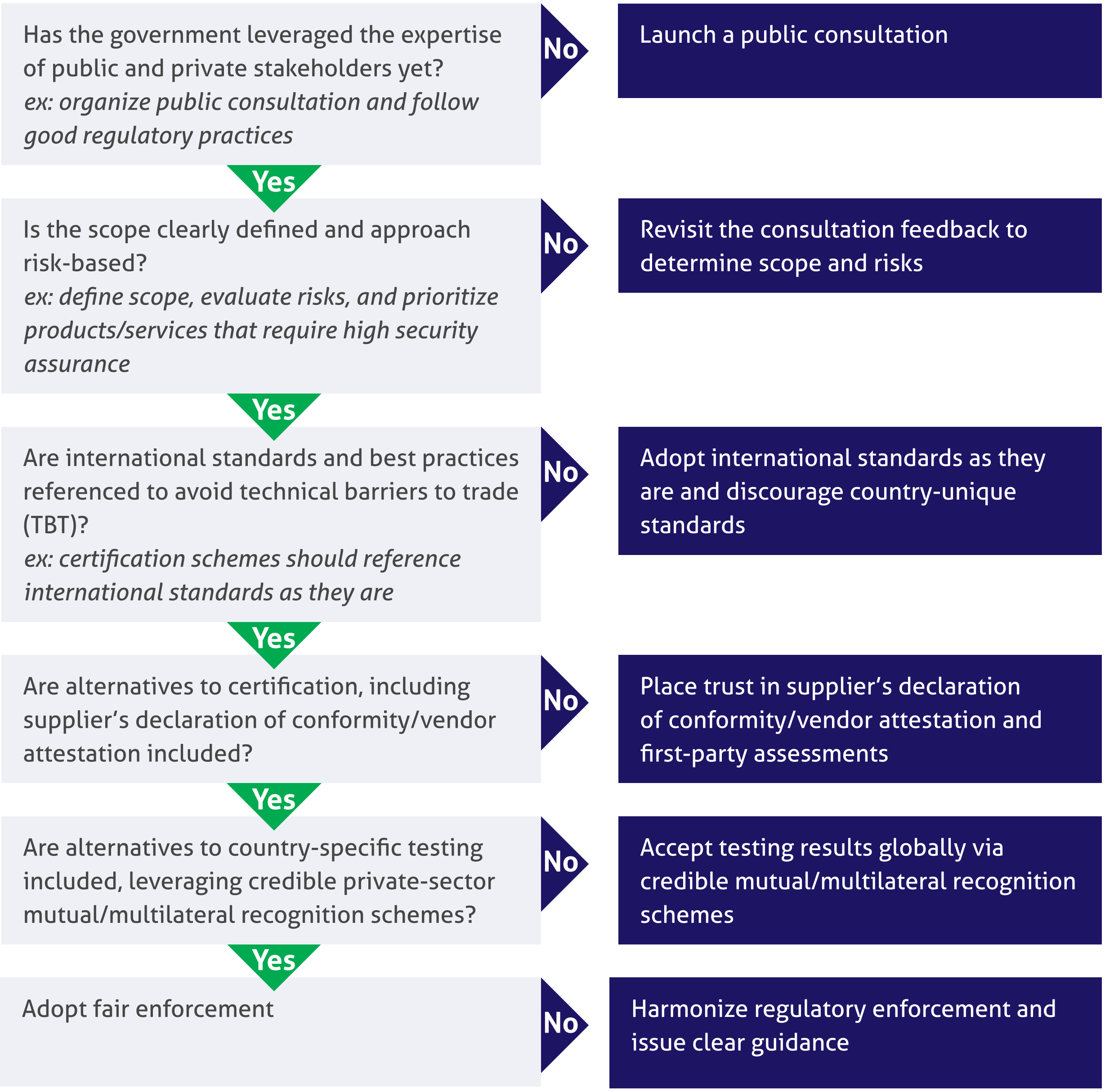
September 2020

ITI Policy Principles for Cybersecurity Certification

Cybersecurity Certification is not a comprehensive solution.

ITI recognizes and respects the governments have the right to propose certifications for cybersecurity. However, policymakers should be aware that certification assessment only reviews information about security at a specific point in time, and ever-evolving cybersecurity is a shared responsibility among vendors, consumers and all parties.

If governments choose to adopt certification schemes...



Has the government leveraged the expertise of public and private stakeholders yet?
ex: organize public consultation and follow good regulatory practices

No → Launch a public consultation

Yes

Is the scope clearly defined and approach risk-based?
ex: define scope, evaluate risks, and prioritize products/services that require high security assurance

No → Revisit the consultation feedback to determine scope and risks

Yes

Are international standards and best practices referenced to avoid technical barriers to trade (TBT)?
ex: certification schemes should reference international standards as they are

No → Adopt international standards as they are and discourage country-unique standards

Yes

Are alternatives to certification, including supplier's declaration of conformity/vendor attestation included?

No → Place trust in supplier's declaration of conformity/vendor attestation and first-party assessments

Yes

Are alternatives to country-specific testing included, leveraging credible private-sector mutual/multilateral recognition schemes?

No → Accept testing results globally via credible mutual/multilateral recognition schemes

Yes

Adopt fair enforcement

No → Harmonize regulatory enforcement and issue clear guidance

September 2020

ITI Policy Principles for Cybersecurity Certification

We understand that some governments around the world are developing cybersecurity certification schemes for products, services, or company processes in an attempt to gain more confidence in product/services/companies in their markets, some of which may be mandatory.

ITI recognizes and respects that governments have the right to prepare, apply, and maintain mandatory regulations for cybersecurity certification. However, policymakers should be aware that certification assessment only reviews information about security at a specific point in time. While certifications can be useful in certain instances, they are not appropriate for all products or in all cases and they only address a discrete aspect of cybersecurity.

Improving cybersecurity requires a multi-faceted approach that includes education, training, and skills development; raising awareness at the executive and board-levels; cyber threat information sharing; promoting a prevention-first mindset; and, for governments, instituting effective legal regimes to deter and prosecute cybercriminals. Governments should emphasize all of these potential levers in their policy responses. Further, governments should recognize that improving cybersecurity is a shared responsibility among all stakeholders. Suppliers/vendors should design and equip products and services with the strongest security in mind, update their products and services, and conduct due diligence in risk management to the extent possible. At the same time, end-users, including businesses and consumers, should recognize that their behavior and specific use/application of a given product is instrumental in contributing to security.

As governments consider regulations to mandate certification to assess cybersecurity risks, we provide the following principles to guide their actions. We also provide, as an annex, definitions of the key concepts in this document.

1 Governments should recognize that certification is not a comprehensive solution for cybersecurity.

- There are limited scenarios where certification could play a useful role: the product is suitable for certification (e.g., an appropriate standard exists against which to certify), and a high level of assurance is required. In these cases, such assessments may provide a level of confidence to consumers and authorities.
- However, certification might not be appropriate for all products or use cases, and governments should always consider alternatives to certification for managing cybersecurity risks. Mandatory certification should be used only in situations where no better alternatives exist. ITI strongly encourages governments to consider the viability of alternative options including education programs, voluntary standards, and first-party assessments.
- Cybersecurity is not an end state. Rather, it is a continuous effort to protect products, services, and uses, based on the latest threat/vulnerability information available using the best available techniques, throughout the deployment lifecycle. Because there is no one-size-fits-all solution to evaluate cybersecurity risks, certification cannot represent a complete picture of security or a "silver bullet solution."
- Certification can often have the opposite result of what was intended and cause lower levels of security as it can encourage the use of older certified versions of products/services or complacency based upon the perception that products and services that are certified are better even when those certifications are outdated.
- Certification can be costly, and resources are finite. Thus, requiring cybersecurity certification could result in undesirable trade-offs, a main one might be stifling innovation.
  - *The monetary tradeoff could preclude some suppliers/vendors from bringing products to market, negatively limiting consumer's/business' choices.*
- Certifications do not necessarily equal security and reduced risk, because certifications are issued at a point in time and therefore only reveal information about security at that specific point in time with that specific configuration profile; further, threats are dynamic and constantly changing. In addition, in many cases, due to the long period of time and effort required to complete a certification, a certified product or service may no longer be at the leading edge of security and may not account for the latest innovations to address ever-evolving cyber threats.
- Mandating certification of certain cybersecurity aspects does not provide absolute confidence or assurance. A cybersecurity certification scheme that is not fit-for-purpose or dynamic can create a false sense of security and undercut the desired improvement in cybersecurity.[1]
- Governments should consider the practices of their ICT vendors, rather than merely focusing on products and services. 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 management.

[1] Tenable. "Tenable Research Reveals Nearly Half of Organizations Use Strategic Vulnerability Assessment as Foundation of Cyber Defense" August 8, 2018.

If governments choose to set regulations and mandate certification schemes:

2 Governments should leverage the expertise of public and private stakeholders and ensure transparency.

- Any government certification schemes should be proposed and adopted through an open and transparent process that allows for adequate time, opportunity, and tools for stakeholder input and public comment. This will allow for refinement at appropriate stages of the policy process in advance of the final adoption.

- Governments should leverage the expertise of all stakeholders, including the private sector, to build upon cybersecurity approaches that exist or are emerging elsewhere. In particular, it is essential to identify how any new certification schemes would not duplicate or contradict existing relevant global schemes, and/or whether equivalency needs to be established between the schemes. Furthermore, it should be established if an existing global scheme addresses the actual risk requirements (or enhanced levels of an existing scheme can be identified) rather than introducing a 'bespoke' scheme.

- Through the adoption of these and other good regulatory practices, governments should promote regulatory quality through greater transparency, objective and evidence-based analysis, accountability and predictability. Transparent communication between policymakers and a broad range of stakeholders alleviates regulatory uncertainty and can prevent the emergence of barriers to trade, as well as facilitating credible decision-making that is based on reliable, high-quality information.

3 Governments should take a risk-based approach and clearly define the scope of certification schemes.

- Any certification schemes should be based on appropriate risk factors. Priority should be given to certification schemes for products, services or processes requiring high security assurance due to their specific use, such as for critical information infrastructure (CII).

  - *A set of common risk factors to evaluate criticality may include intended end use, operating environment, data collected and functionality, among other characteristics.*

  - *Context is key. For example, products and services that are intended for home use should not be treated the same as products and services intended for national security purposes. Time-consuming and expensive certifications may be viable in some contexts related to critical infrastructure protection but are likely ill-suited to consumer products with short life spans and multiple use contexts.*

- Because there is no one-size fits all product certification scheme that can apply across a wide array of ICT technologies, governments should take efforts to clarify which technologies should appropriately be considered in scope. A narrowed scope is particularly important to ensure success for all stakeholders. Governments should also consider if it is appropriate to certify the product or more appropriate to achieve a level of confidence and trust in the vendor and their ecosystem.

- Products, inclusive of their ecosystem (e.g., technologies, supporting processes) should be able to maintain a current certification status without requiring re-certification until either the product undergoes a major change impacting risk (based on defined criteria for a major change) or the certification period ends; conversely, if the certification period ends but the product hasn't undergone any major changes and the certification requirements are still the same, then it should be possible to extend the validity of the certification with minimal efforts. For services, the choice between maintaining certification status versus updating and patching systems can be at odds. Conformity assessment programs should not disincentivize or penalize security updates or innovation, therefore, alternatives to certification programs for services (that pose high risks) need to be strongly considered.

- Governments should consider the adoption of an equivalency process for other certification programs that they view are at or above the same risk mitigation level.

- If a certification program is deemed to be the only appropriate answer then that scheme must be dynamic and the time, cost and complexity of completion must be commensurate with the security target, need for evolution and adoption.

4 Governments should reference international, industry-led standards and best practices as the technical basis for certification to avoid technical trade barriers.

- To support innovation and promote interoperability in cybersecurity, governments should support open, transparent, industry-driven, consensus-based international standards.

- When deemed necessary based on risk, cybersecurity certification schemes should be grounded in international, industry-led, voluntary consensus standards and best practices. ITI encourages governments to reference such standards as they are written and published as the technical basis for certification schemes, which will facilitate innovation and prevent the emergence of damaging technical barriers to trade (TBT).

- We support full adoption of international standards and discourage creation of country-unique standards. Unwarranted deviations from international standards can have a serious effect on trade, such as requiring suppliers to meet different technical specifications, forcing unnecessary duplication of testing and requirements, delaying the entry of goods into market, adding costs and reducing the availability of products and services to the population, and inevitably reducing innovation and competition.

    - *While there are differences in policy and regulatory regimes across regions rendering full harmonization unlikely, substantial benefits are still possible if international standards (with no deviations or only justified deviations/elevations) serves as the basis of regulations.*

- In terms of process standards, each sector may have unique cybersecurity standards, but there are a set of cybersecurity controls that are common and can be applied based upon risk across sectors. We recommend that governments reference commonly used process standards in the ICT space such as the ISO/IEC 27000 series and the IEC62443 suite of standards, in addition to looking, where appropriate, to industry-leading standards developed in organizations such as the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF) and the

Organization for the Advancement of Structured Information Standards (OASIS). Pointing to such international standards provides a basis for harmonization and alignment across countries.

- Any regulatory schemes should be technology neutral and refrain from mandating prescriptive technical features/controls as they can become outdated quickly and be at odds with the basic economics of product and services design. International standards that have performance-based requirements that take risk into account should be preferred.

5 Governments should consider alternatives to certification, such as supplier's declaration of conformity/vendor attestation.

- Alternatives to certification are widely accepted in the marketplace, depending on the product, service, use, or standard—and risk. These alternative approaches to demonstrating compliance are used by vendors, recognized and accepted by the marketplace, and are ones in which industry has extensive experience. They also respond to the need for flexibility, agility, and cost limits that must be borne by vendors (and, ultimately, purchasers). The appropriate method to demonstrate compliance should be chosen depending on the level of risk deemed acceptable.

- In many instances, certifications may be the least desirable mechanism, particularly where the assessment of dynamic cybersecurity risks is concerned. Third-parties only have visibility into the security of a product at a single point in time and the evaluation and certification processes often take a long time, therefore potentially negatively impacting security in those cases where organizations or suppliers/vendors frequently deploy security updates.

- Examples of alternative means of attestation include supplier's declaration of conformity (SDoC) and vendor attestation.

- Where deemed appropriate by risk-based analysis, we encourage governments to trust in SDoC or vendor's attestation for many, if not most, technologies and their expected uses, because suppliers/vendors maintain end-to-end visibility of the security of their products and services and are best situated to identify a combination of standards that address their specific risk profiles and business models. Such agile approaches are underpinned by international standards for SDoC (ISO/IEC 17050 part 1 & 2) and enable companies of all sizes to more rapidly deploy tools to address cybersecurity challenges.

- Governments should consider acceptance of first-party assessments, in which a separate and independent function from the design team conducts an internal assessment of a company or entity's own products and services. Such assessments are functionally comparable to third-party assessments, providing confidence while adding the benefit of the company's extensive familiarity with the product, services, and related processes.

- First-party assessments promotes accountability by the supplier of a product or service who can provide relevant documentation required by market surveillance authorities.

6 Governments should recognize supplier/vendor assessments and labs, avoid localized testing and leverage mutual/multilateral recognition schemes.

- Governments should accept supplier/vendor assessments, and they should accept supplier/vendor assessments by competent testing laboratories owned by supplier/vendor, on terms no less favorable than those owned by a third-party, even when the testing laboratories are in a foreign territory.
    - *Mandated third-party assessments or localized testing and geographic limitations on which labs may be designated to carry out cybersecurity certification can bring significant capacity constraints and corresponding backlogs in the deployment of cybersecurity tools and solutions.*
- Governments should leverage credible private-sector mutual/multilateral recognition schemes, such as the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement, the International Accreditation Forum (IAF) Multilateral Recognition Arrangements (MLA), and the Common Criteria Recognition Arrangement (CCRA).
- Where necessary, governments may also pursue Mutual Recognition Agreements (MRAs), which, while less efficient than reliance on other approaches that facilitate the acceptance of international certification results, are functional mechanisms to enable acceptance of certification test results, reduce trade barriers, and allow deployment of timely cybersecurity solutions on the market.

7 Governments should adopt fair enforcement.

- ITI supports the role of governments or a designated authority in fairly conducting effective and focused enforcement activities to ensure that products and services are complying with stated requirements.
- Governments should ensure there is clear, efficient, harmonized regulatory enforcement and guidance to help accelerate industry adoption for schemes, including appropriate market surveillance.
- Penalty-setting should be governed by the principle of proportionality. Enforcement activities should not have the effect of punishing those least likely to cause problems.

Appendix A: Glossary

Term	Definition	Source
Attestation	Issue of a statement, based on a decision following review, that fulfillment of specified requirements has been demonstrated *NOTE 1 The resulting statement, referred to in this International Standard as a "statement of conformity", conveys the assurance that the specified requirements have been fulfilled.* *NOTE 2 First-party and third-party attestation activities are distinguished by the terms declaration [first- party] and certification [third-party].*	ISO/IEC 17000
Certification	Third-party attestation related to products, processes, systems or persons.	ISO/IEC 17000
Conformity Assessment	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.	ISO/IEC 17000
First-Party Assessment (also known as self-assessment)	Conformity assessment activity that is performed by the person or organization that provides the object.	ISO/IEC 17000
Supplier Declaration of Conformity (SDoC) (also known as Manufacturer Declaration of Conformity)	First-party attestation NOTE 1 "Supplier's declaration of conformity" is a "declaration" as defined in ISO/IEC 17000, i.e. first-party attestation.	ISO/IEC 17050
Testing	Determination of one or more characteristics of an object of conformity assessment, according to a procedure.	ISO/IEC 17000
Third-Party Assessment	conformity assessment activity that is performed by a person or body that is independent of the person or organization that provides the object, and of user interests in that object.	ISO/IEC 17000