

Trusted Technology Provider Framework

ACS Program Overview & Update

v1.3

“Build with Integrity
Buy with Confidence”

Andras R. Szakal,
IBM Distinguished Engineer, Director IBM Federal SWG
aszakal@us.ibm.com
Chair Trusted Technology Forum

Note: TTFP Materials are copyrights of The Open Group
All information presented is WG draft and subject to change



Need to Work Together to Develop Expectations for a Commercial off the Shelf (COTS) Product

- “Good Commercial Product” – Helpful information that builds understanding of the product
 - What’s in it (source code and origin/pedigree)
 - Who built it (development and manufacturing)
 - How will it be sustained from an OEM perspective
 - What were the management, process and quality controls applied
 - What are the meaningful supply chain considerations
 - What variability, and volatility of sub-processes and supply should be expected (opportunistic component sourcing and contract fabrication)
 - What other “measures of goodness” can be used or leveraged
 - Not a substitute for ISO, NIST, or ITU; Interoperability or protocol level compliance or certification

What is
Realistic
Consumable
Affordable
Best
Practices

Government /
CKI
Expectations

Collaborating with the IT Industry

- Need to understand: What is a “Good Commercial Product”
 - **Multiple efforts** (many still ongoing) by Government to prescribe standards for strength of IT security products, e.g. FIPS, Common Criteria. This assumes that products are designed and developed to meet established criteria. What if our goal is to simply acquire “good commercial products?” What do you consider to be a “good commercial product”
 - **WW Consumers** seek lower cost/higher performance commercial building blocks for secure systems and systems of systems (SoS)
 - **Industry can benefit immensely:**
 - Qualitative brand differentiation
 - Taking credit for existing corporate best practices
 - Common interfaces promote lower cost interoperability
 - Opportunity to define and dispel globalization concerns

“Build with Integrity
Buy with Confidence”

What Problems Are We Solving?

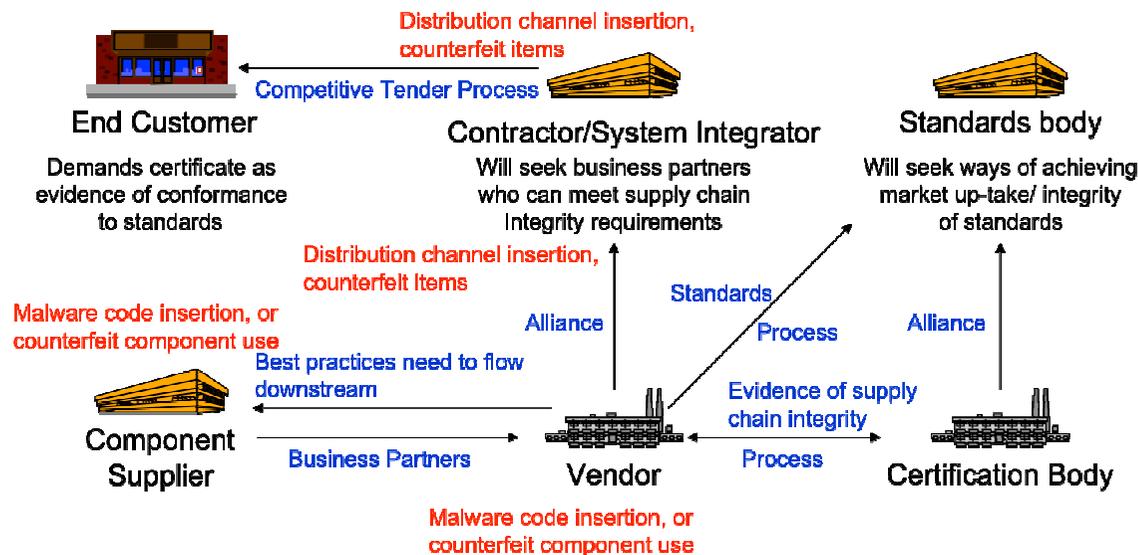
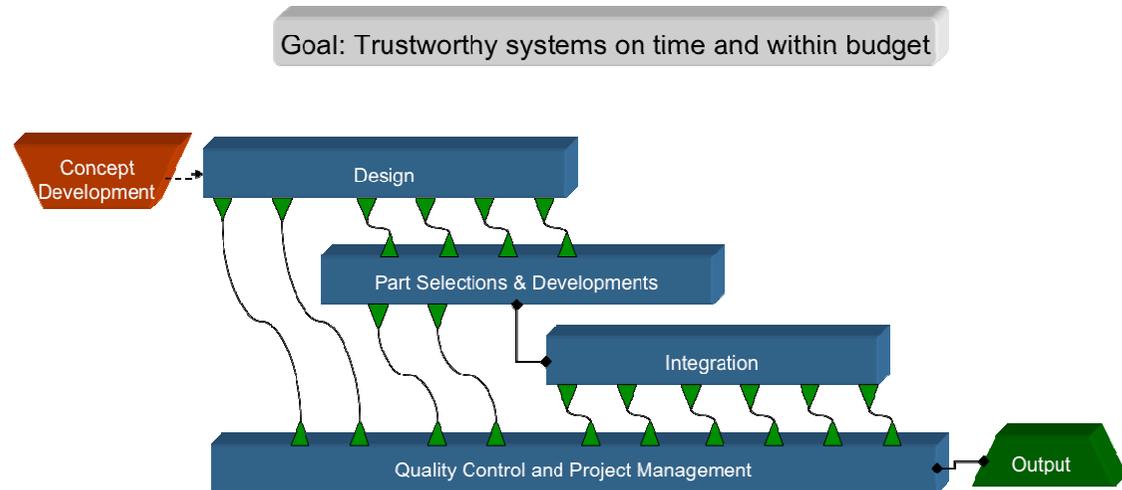
- Consumers seek to reduce the cost, acquisition time, and risk to critical systems through leverage of commercial products and technologies:
 - What **potential integrity risk** may be inherited from supply chains, both for software and hardware, and how the original equipment manufacturer (OEM) assesses and manages these risks?;
 - Practices that can **mitigate potential risks** of significant supply chain attacks;
 - Risks to confidentiality, integrity, and availability to a customers environment or critical infrastructure as a result of procurement by customers of **counterfeit components and products**;
 - What software or technology **development or engineering practices** can help reduce product integrity risks?;
 - How is product assurance and risk managed through the adoption of **industry best practices and recognized international and open industry standard?**

Technology Industry Led Approach

- Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices:
 - **Identify product assurance practices** that should be expected from all commercial technology suppliers based on the baseline best practices of leading trusted commercial technology suppliers
 - Help **establish expectations for global government and commercial customers** when seeking to identify a trusted technology supplier
 - **Leverage existing** globally recognized information assurance practices and **standards**
 - Share with commercial technology consumers secure manufacturing and **trustworthy technology supplier best practices**
 - **Harmonize language** used to describe best practices

ACS-I Deliverables / Success

- Developed Business Scenario White Paper
- Defined Ecosystem
- Pain Points
- Problem to be solved
- Published TTPF
- Operational Vision



➤ Mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

Trusted Technology Forum Vision / Mission / Principles

TTF Vision:

- We are a global consortium established to support the adoption of best practices for secure technology engineering and procurement strategies in order to develop a more trustworthy global technology supply chain.

TTF Mission:

- The Trusted Technology Forum is an open, vendor-neutral initiative that formulates and supports use of a global framework, guidelines, procurement strategies and related resources that can
- Help the technology industry “*build with integrity*”
- Enable customers to buy with confidence; and
- Support global innovation.

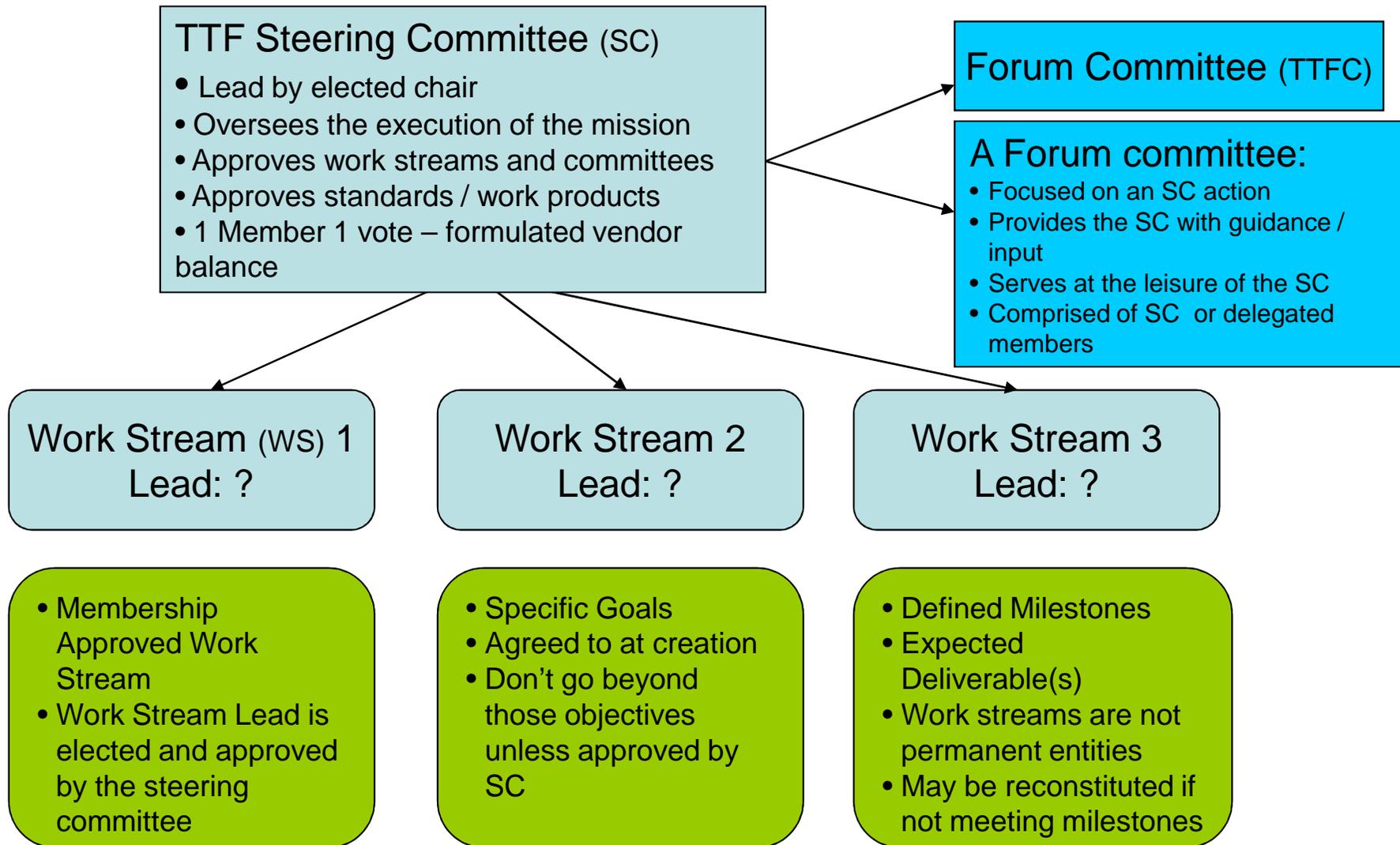
TTF Standards Principles

Principles for accomplishing our mission:

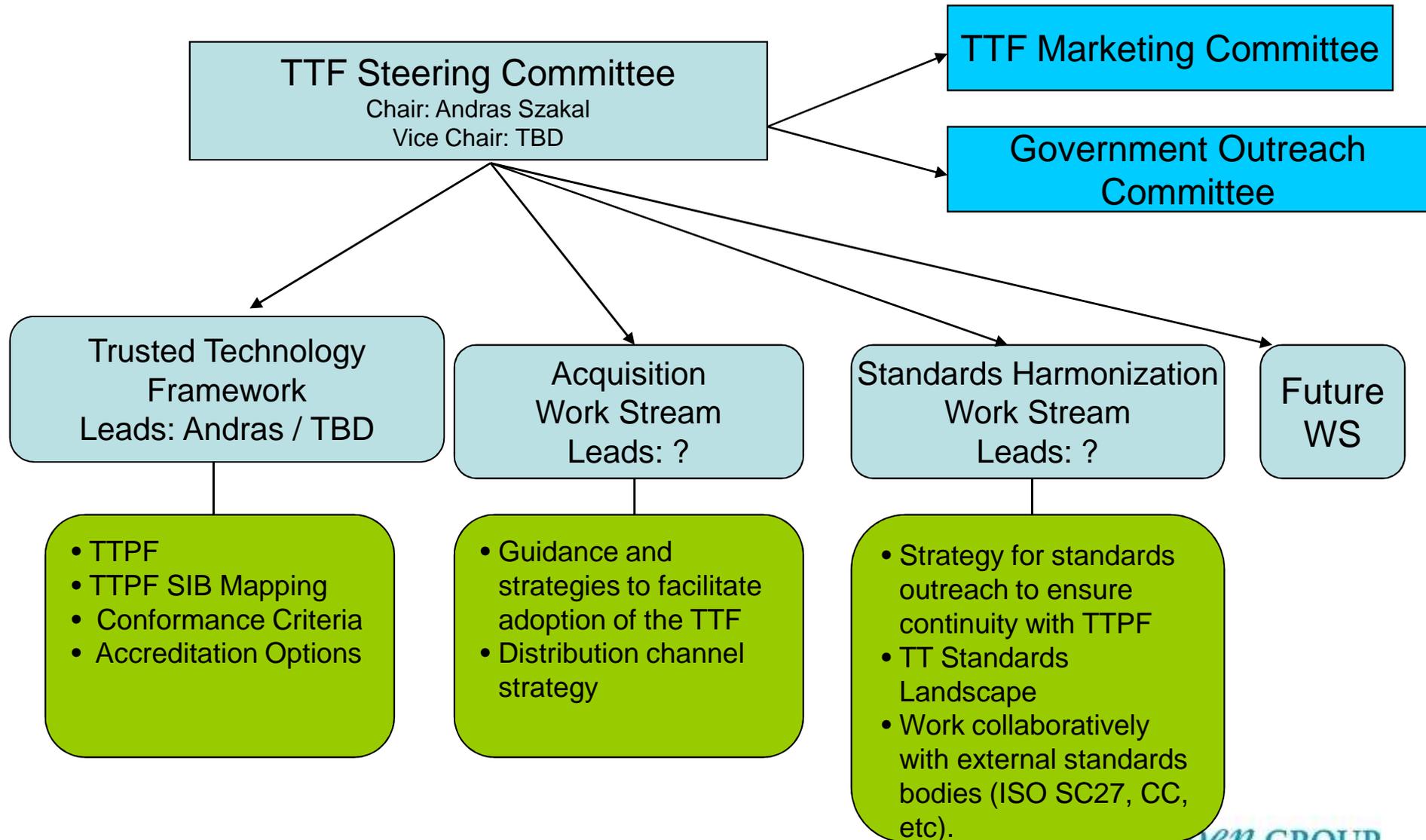
Our mission will be accomplished by providing vendors, distributors, integrators and consumers commercially reasonable integrity practices that are;

- **Practical and effective** – Practitioner based, evidence that it works in the field
- **Reasonable** – Achievable and implementable by a wide variety of vendors and stakeholders
- **Affordable** – Reasonably cost effective to implement
- **Open** – Based on open standards and recognized industry best practices

TTF Governing Structure



TTF Governing Structure (Current WS and Committees)



TTF Milestones

- Completed review of ACS-I final deliverables
- Launched new Trusted Technology Forum
 - Membership
 - Structure of the TTF / Governance
 - Initial Work Streams
 - Media
 - Government Outreach
 - Following the TOG standards process to finalize public release of initial TTPF white paper
- Current activities
 - 3 Work streams – TTPF, Acquisition, Standards Harmonization
 - Complete formal review of TTPF – target is Feb member meeting in San Deigo

Trusted Technology Provider Definitions

- **Supply Chain Attack (general)**

In general, a supply chain attack is an attempt to disrupt the creation of goods by subverting a commercial manufacturing, ordering, or distribution process.

- **Supply Chain Integrity**

The manufacturing and/or development process performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation. Extends NIST definition [NIST 800-12].[\[1\]](#)

- **Technology Supply Chain Attack**

A technology supply chain attack subverts the hardware, software, or configuration of a product, prior to customer delivery, for the purpose of introducing an exploitable vulnerability.

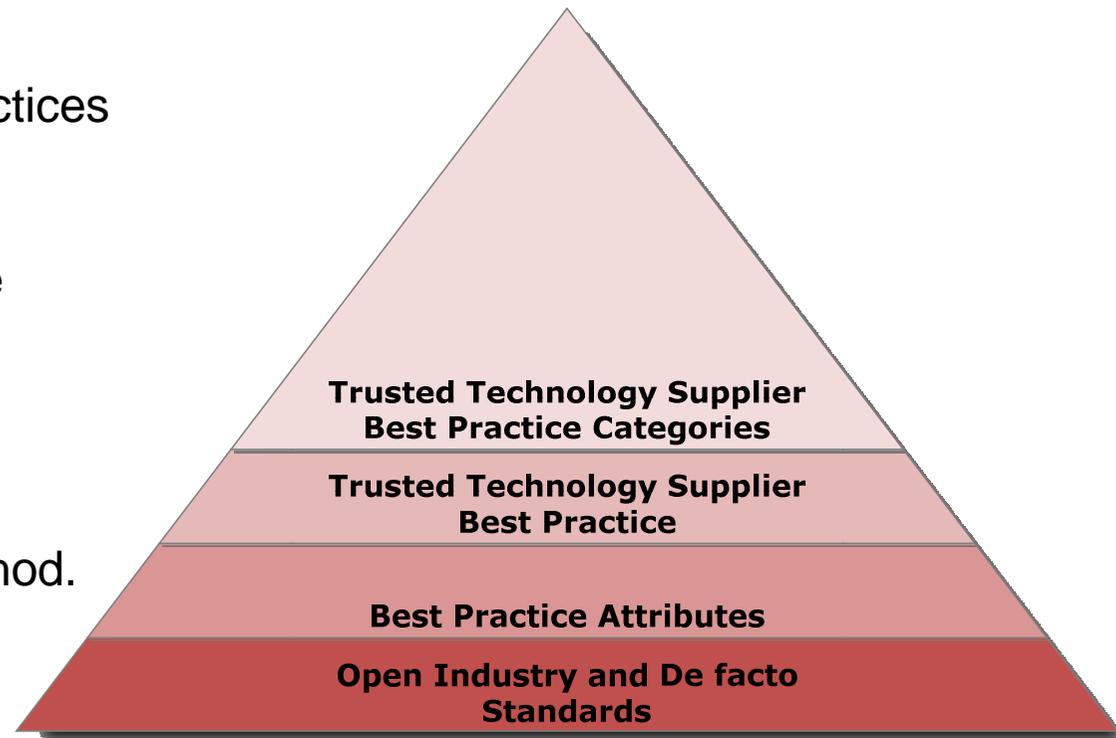
- **Technology Supply Chain**

The manufacturing and/or development process used to produce and deliver hardware or software technology products and their configuration.

[\[1\]](#) NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook; refer to: <http://csrc.nist.gov/publications/PubsSPs.html>.

Trusted Technology Provider Framework

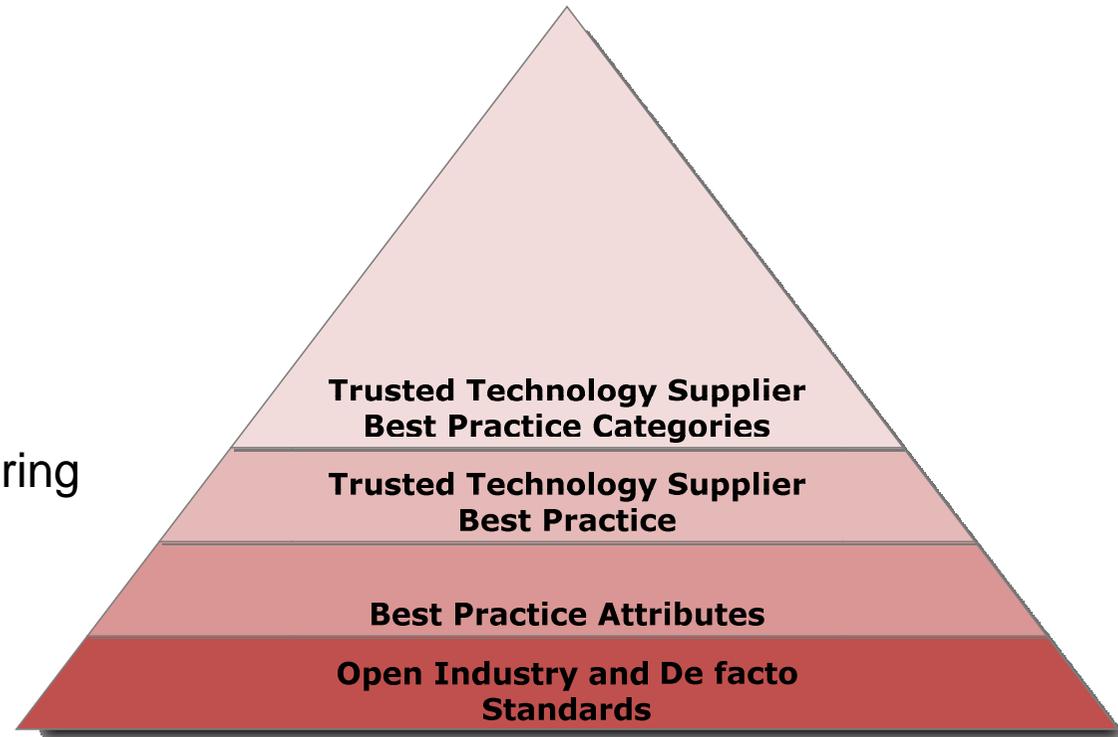
- Grouping of industry best practices by category.
- Best practices of most mature industry technology vendors
- For example, a supplier implements a Secure Engineering/Development Method.
- Simple but not simplistic
- Realistic, consumable, actionable for technology vendors in a global environment



Trusted Technology Provider Framework

The framework is broken into categories of Industry Best Practices:

- Development / Engineering Practices
- Secure Development / Engineering
- Supply Chain Integrity
- Product Evaluation Practices



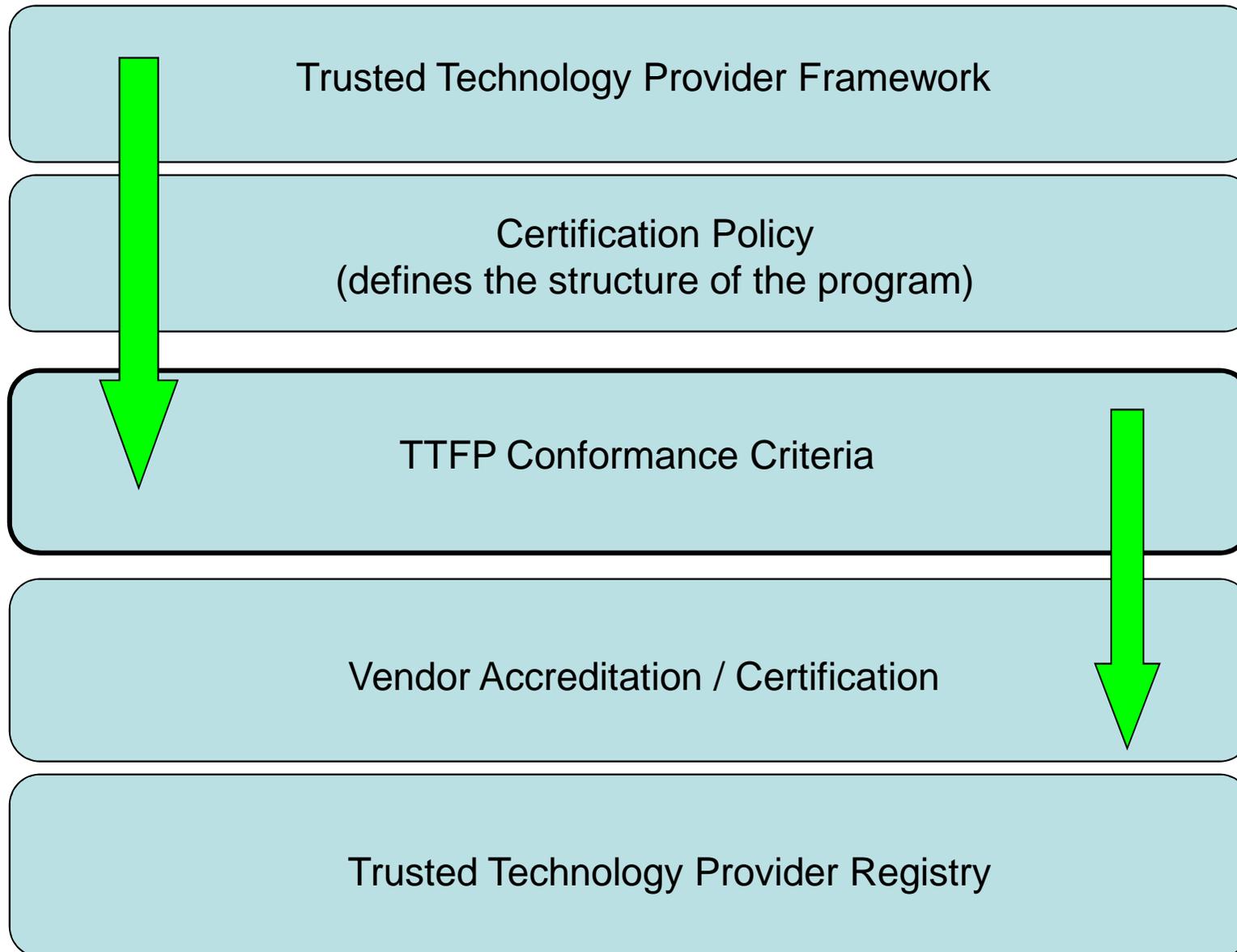
TTPF Best Practice Categories

Best Practice Categories	Definition
Product Engineering / Development Method	Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.
Secure Engineering / Development Method	Trusted Technology Suppliers employ a security engineering method in designing and developing their products. Software vendors often employ methods or process with the objective of identifying, detecting, fixing, and mitigating defects and vulnerabilities that could be exploited, as well as, verify the security and resiliency of the finished products. Hardware vendors may also include ways to mitigate use of unverified and inauthentic software and protection for counterfeit hardware or software,
Supply Chain Management Method	Trusted Technology Suppliers manage their supply chains through the application of defined, monitored and validated supply chain processes. These practices seek to ensure the integrity of the supply chain throughout product design, sourcing, fabrication delivery, support and end-of-life.
Product Evaluation Method	Common Criteria currently evaluates products, comparing actual performance to claimed capabilities. Trusted Technology Suppliers utilize Common Criteria and other industry or governmental testing certifications, to help validate product integrity.

Example TTPF Best Practice and Guidance

Industry Best Practice	Guidance
<p>Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.</p>	<p>Engineering/development methods are practical and meaningful within the vendor’s domain of software, firmware, or hardware manufacturing. This can be measured in the following ways:</p> <ol style="list-style-type: none"> 1. The method must be demonstrably successful in practice. Successful means two things: <ul style="list-style-type: none"> • When used correctly, the method routinely has the effects it claims to provide. • The results satisfy the needs of the method’s constituencies. 2. The method is maintained by an active community of practitioners. 3. The method must have explicitly defined inputs, participants, roles, process steps, outputs, results, and deliverables. 4. The method must be supported by self-paced or instructor-led training to a published, common curriculum. 5. The method must be supported by collateral materials for use by practitioners. These materials might include, for example, templates, tools, examples, and best practice recommendations. 6. The method must have a defined process for feedback from practitioners and the maintenance and revision of the above materials (community, documentation, training, and collateral). 7. The method supports the defined attributes of a well formed engineering/development method as defined in Secure Engineering/Development Method.

Envisioned Trusted Technology Provider Program



Example TTPF Conformance Requirements

Industry Best Practice	Notes
Trusted technology providers utilize and internalize the application of a well-formed and documented development or manufacturing method or process.	Engineering/development methods are practical and meaningful within the vendor's domain of software, firmware, or hardware manufacturing as defined by the TTPF Method Guidance.

Best Practice Attribute	Attribute Definition
Requirements Management	Requirements are documented and traced back to product functionality.

Example Conformance Criteria

The Technology Provider documents product functional and non-functional requirements. Requirements can be traced back to implemented function. Evidence can be provided in the form of an electronic repository or paper document that describes where a requirement is realized in product function.

TTPF Conformance Requirements

Category: Product Engineering / Development

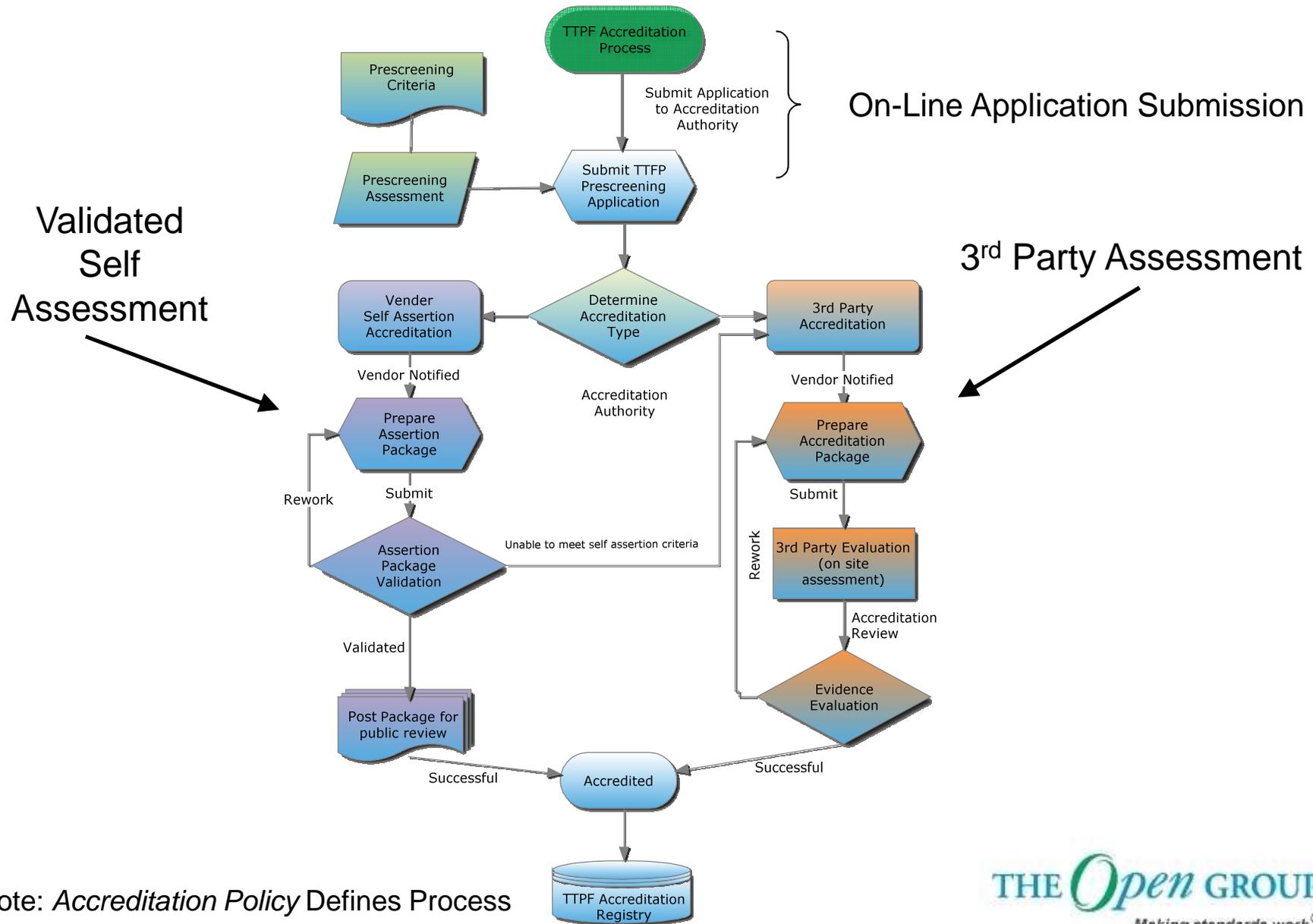
TTPF Mapping	Conformance Statement	Evidence Requirements
Product Engineering/ Development Method	Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.	Applicant must provide evidence of the use of a meaningful method as defined by the method recognition criteria. {As defined by TTPF Method Guidance}
Product Engineering / Development Method	Product engineering methods are specified and refined to best fit the engineering / development characteristics of the target product.	Applicant must explain: a. How the method meets the needs of the engineering/ development team. b. How the method has been refined to meet the characteristics of the target product.
Product Engineering / Development Method Requirements Management	Product requirements are documented and traced back to implemented product functionality. Product functionality are traced back to functional requirements.	Applicant provides example of documented product requirements and traceability matrix (or equivalent).
Product Engineering / Development Method Formal Product Engineering or Development Community	Product lifecycle practices and processes are supported by a community of practitioners who vigilantly maintain the organization's engineering practices.	Applicant provides evidence that engineering / development practices are maintained, evolve and grow through the feedback and contributions of a community of practitioners.

NOTE: For Use as Example Only

TTPF Marked Program Assumptions / Decisions

- Assumption: Program Design
 - Focused on consumability, scalability with highest possible degree of validity
- Assumption: Use of term Accreditation
 - Certification is overloaded and conflicts with CC
- Assumption: TTPF Accreditation
 - Currently using TTPF Accreditation as working name
 - Need to agree on formal name
- Assumption: Initially Open Group is the Certification Authority
 - Future program may establish 3rd party accreditation to facilitate growth

Strawman TTPF Accreditation Process



Note: Accreditation Policy Defines Process

Thank You!

If you would like to participate in evolving this set of best practices and in helping to shape how this set of best practices will be used to indicate trustworthy products, and allow suppliers to “Build with Integrity” and governments and commercial entities as well to “Buy with Confidence”, please contact Mike Hickey at: m.hickey@opengroup.org.