This document is a product of the IGQ Working Group of TIA QuEST Forum. It is subject to change by the IGQ Working Group with the latest version always appearing here.

SCS Status Assessment Measurements

Background: A group of international experts on the ICT supply chain, under the auspices of TIA QuEST Forum, has developed this list of the Top 25 Supply Chain Security Measurements to challenge members, partners, the ICT industry, and the supply chain of other critical infrastructures.

Purpose: This list is intended to be a tool that allows organizations to assess the security status of their supply chain, both externally and internally.

Usage: A user of this tool, would engage with their internal and external stakeholders to establish key datasets to collect and calculate these measures. For some measurements, a result of 0% is the best, for other measurements 100% is best. They could be measured across individual business units and across the enterprise for comparison.

Validation: Trust but Verify: As with all measurement programs, you must always verify the integrity of the numbers, never trust a single report or someone's assumptions.

Scope: The scope of your evaluation is always be based on ALL elements of your company (e.g., ALL suppliers, ALL systems, ALL buildings). But if there is a need to evaluate these at a smaller scope (e.g., All suppliers under a single division) then the results should be footnoted to make sure the audience is aware of this reduced scope. Remember cloud provider A presents risks to your assets and supply chain but so does Billy Bob the Plant Waterer, LLC, he also impacts the risks to your assets and supply chain.

Definitions:

Supplier, third party, vendor – any external entity that you get products or services from, that impact the risk to the company, regardless of whether you pay them directly or indirectly and regardless of whether you have them under contract or not.

Personnel – individuals, whether employees, supplier/third party/vendor employees

Software – Firmware, disk-based software, cloud-based software, operating system level, data base level, application level, etc.

Subcontractors - any external entity, that is used by your direct suppliers, that you get products or services from, that impact the risk to the company, regardless of whether you pay them directly or indirectly and regardless of whether you have them under contract or not.

Audience: You, Audit Team, Security Team, Sourcing/Procurement Teams, Executives, Your Suppliers

TIA Top 25 Supply Chain Security Measurements – 2021 Edition

	The Measure	Best Score
1	Percentage of our suppliers that have contractual required security requirements	100%
2	Percentage of third-party software installed in our environment, that is end-of-life	0%
3	Percentage of third-party software installed in our environment that has all security patches installed	100%
4	Percentage of personnel (non-employees) with access to our email environment, that passed our phish test	100%
5	Percentage of third party managed, internet facing devices, monitored 24x7 for security incidents	100%
6	Percentage of proprietary internal software, developed by third parties, that has been through a automate and human code review	100%
7	Percentage of third-party managed buildings with our assets, that doesn't have cameras, access control covering our assets.	0%
8	Percentage of our systems/applications that have suppliers managing the security controls	0%
9	Percentage of suppliers that have access to our data, that haven't been assessed/audited onsite by our auditors and security teams	0%
10	Percentage of supplier employees accessing our network from unauthorized (per contract) locations	0%
11	Percentage of suppliers that use subcontractors with physical or electronic access to our assets	0%
12	Percentage of supplier employees with access to our assets, that haven't had a human verified background check / chemical test (as allowed by law)……in the last XX years	0%
13	Percentage of COTS devices on internal network, that are managed, in inventory, with a named owner	100%
14	Percentage of suppliers that have been screened against sanctions listings	100%
15	Percentage of third-party managed email domains supporting, our organization controlled, by DKIM	100%
16	Percentage of third-party managed DNS servers supporting our organization with DNSSEC implemented	100%
17	Percentage of supplier employees protecting our environment by performing security functions, not defined in their contract	0%
18	Percentage of suppliers that have 24x7 incident response contacts in our CSO/CISO's IR program database	100%
19	Percentage of suppliers that support our business and government customers, that we have verified onsite, are fully compliant with the flow down security requirements	100%
20	Percentage of third parties with physical and/or electronic access to our environment, that is covered by our insider threat monitoring capabilities	100%
21	Percentage of supplier hosted data where access reporting timelines are verifiably within regulatory maximums	100%
22	Percentage of third-party providers that manage security (physical or logical) without contractual managed CPIs/KPIs	0%
23	Percentage of shipments (inbound, outbound, third party products, our products) that aren't providing real time GPS/RTK package tracking	0%
24	Percentage of suppliers without a financial stability report on file with us, within last ## years	0%
25	Percentage of suppliers that impact our business continuity, that have no documented & tested business continuity plan	0%